# User Manual

## 13.0

# MDaemon Messaging Server
# User Manual

Copyright © 1996-2012 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

v13.0.0 - September 2012

# Table of Contents


## Section I MDaemon Messaging Server 13.0 12

1 Introduction ... 12
- MDaemon Features ... 13
- System Requirements ... 15

2 New in MDaemon 13.0 ... 15

3 Getting Help ... 22

## Section II Upgrading to MDaemon 13.0 26

## Section III MDaemon's Main Display 30

1 Stats ... 30

2 Event Tracking and Logging ... 31
- Event Tracking Window's Shortcut Menu ... 34

3 Composite Log View ... 34

4 Tray Icon ... 34
- Shortcut Menu ... 35
- Locking/Unlocking MDaemon's Main Interface ... 36

5 Session Window ... 36

6 MDaemon's SMTP Work Flow ... 37

## Section IV Setup Menu 40

1 Default Domain / Servers ... 40
- Default Domain & Servers ... 40
  - Domain ... 41
  - Delivery ... 43
  - Servers ... 46
  - Ports ... 49
  - DNS ... 51
  - Timeouts ... 53
  - Sessions ... 55
- Mail Release ... 57
  - On-Demand Mail Relay (ODMR) ... 59
- Archiving ... 59
- Pruning ... 61
- Unknown Mail ... 63
- Domain Sharing ... 64
- Priority Mail ... 66
- IP Cache ... 68
- Header Translation ... 70
  - Header Translation Exceptions ... 71
- Domain Signatures (text/plain) ... 72
- Domain Signatures (text/html) ... 73
- Public & Shared Folders ... 74
  - Public & Shared Folders ... 75


*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Folder Listing ... 77
Access Control List ... 79
**DomainPOP ... 81**
Host & Options ... 83
Parsing ... 85
Processing ... 87
Routing ... 88
Foreign Mail ... 89
Name Matching ... 90
Archive ... 92
**RAS Dialup Settings ... 92**
RAS ... 93
Logon ... 94
Processing ... 95
**LDAP/Address Book Options ... 96**
LDAP ... 97
**Logging ... 99**
Log Mode ... 99
Composite Log ... 101
Windows Event Log ... 102
Maintenance ... 103
Options ... 104
**2 Domain Manager ... 108**
**3 Web & IM Services ... 111**
**WorldClient (web mail) ... 111**
Overview ... 111
Calendar & Scheduling System ... 112
ComAgent ... 112
ComAgent's Instant Messaging System ... 113
Automatic Address Book Synchronization ... 114
Using WorldClient ... 115
WorldClient (web mail) ... 116
Web Server ... 116
Running WorldClient under IIS6 ... 118
SSL & HTTPS ... 121
ComAgent/IM ... 124
Calendar ... 125
Free/Busy Options ... 126
RelayFax ... 127
Options ... 129
**WebAdmin (web configuration) ... 132**
Web Server ... 134
SSL & HTTPS ... 136
Running WebAdmin under IIS ... 138
**Attachment Linking ... 142**
**4 Event Scheduling ... 145**
**Mail Scheduling Options ... 145**
Mail Schedule ... 148
MultiPOP Collection ... 150
**AntiVirus Updates ... 151**
AntiVirus Update Schedule ... 152
**5 Mobile Device Management ... 154**
**ActiveSync ... 154**

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Server ... 154
Policies ... 156
Domains ... 159
Integrated Accounts ... 160
Options ... 161
**BlackBerry Enterprise Server ... 162**
Status ... 166
Policies ... 167
Domains ... 174
MDS-CS ... 175
Integrated Accounts ... 176
Backup/Restore ... 177
Options ... 179
**BlackBerry Internet Service ... 183**
Domains ... 185
Integrated Accounts ... 187
Options ... 189
**SyncML ... 191**
Configuring Your SyncML Clients ... 192
**6 Preferences ... 193**
**Preferences ... 193**
GUI ... 193
System ... 195
Disk ... 197
Fixes ... 199
Headers ... 200
Miscellaneous ... 202
**Windows Service ... 205**
**Section V Security Menu 208**
**1 Content Filter and AntiVirus ... 210**
**Content Filter Editor ... 212**
Rules ... 212
Creating a New Content Filter Rule ... 214
Modifying an Existing Content Filter Rule ... 218
Using Regular Expressions in Your Filter Rules ... 218
Attachments ... 223
Notifications ... 224
Message Macros ... 225
Recipients ... 227
Compression ... 228
**AntiVirus ... 231**
AntiVirus ... 231
AV Updater ... 233
Updater Configuration Dialog ... 235
**2 Outbreak Protection ... 236**
**3 Spam Filter ... 241**
**Spam Filter ... 241**
Spam Filter ... 242
Bayesian Classification ... 245
Bayesian Auto-learning ... 249
Spam Daemon (MDSpamD) ... 251

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

White List (automatic) ... 253
White List (no filtering) ... 256
White List (by recipient) ... 257
White List (by sender) ... 258
Black List (by sender) ... 259
Updates ... 260
Reporting ... 261
Options ... 262
**DNS Black Lists (DNS-BL) ... 264**
Hosts ... 265
White List ... 266
Options ... 267
Auto-generating a Spam Folder and Filter ... 269
**Spam Honeypots ... 270**
**4 Security Settings ... 271**
**Security Settings ... 271**
Relay Control ... 271
IP Shield ... 273
Reverse Lookup ... 275
POP Before SMTP ... 278
Trusted Hosts ... 279
**Sender Authentication ... 280**
SMTP Authentication ... 280
SPF & Sender ID ... 282
DomainKeys Identified Mail ... 284
DKIM Verification ... 285
DKIM Signing ... 289
DKIM Options ... 292
Message Certification ... 294
VBR Certification ... 296
Approved List ... 298
**Screening ... 299**
Sender Blacklist ... 299
Recipient Blacklist ... 301
IP Screen ... 302
Host Screen ... 304
Dynamic Screen ... 306
**SSL & TLS ... 309**
MDaemon ... 310
WorldClient ... 313
WebAdmin ... 316
STARTTLS White List ... 319
STARTTLS Required List ... 320
Creating and Using SSL Certificates ... 320
Creating a Certificate ... 320
Using Certificates Issued by a 3rd party ... 320
**Other ... 322**
Backscatter Protection - Overview ... 322
Backscatter Protection ... 323
Bandwidth Throttling - Overview ... 325
Bandwidth Throttling ... 326
Tarpitting ... 328
Greylisting ... 330
HashCash ... 333

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

LAN Domains ... 335
LAN IPs ... 336
Site Policy ... 337

# Section VI Accounts Menu 340

## 1 Account Manager ... 340

**Account Editor ... 343**
Account Details ... 343
Mail Services ... 345
Web Services ... 346
Folder, Attachments, Groups ... 349
BlackBerry Enterprise Server ... 351
BlackBerry Internet Service ... 353
ActiveSync ... 355
IMAP Filters ... 356
Autoresponder ... 359
Forwarding ... 362
Restrictions ... 364
Quotas ... 366
Aliases ... 368
MultiPOP ... 369
Shared Folders ... 371
Access Control List ... 373
Signature ... 375
Administrator Notes ... 376
Options ... 377

## 2 Account Settings ... 380

**New Account Defaults ... 380**
Mailbox ... 380
Template Macros ... 383
Quotas ... 385
Web Services ... 387
**Autoresponders ... 390**
Accounts ... 390
White List ... 391
Options ... 392
Creating Auto Response Scripts ... 393
Auto Response Script Samples ... 396
**Address Aliases ... 398**
Aliases ... 398
Options ... 400
**Active Directory ... 402**
Monitoring ... 404
Options ... 406
**Outlook Connector for MDaemon ... 408**
Outlook Connector Options ... 409
Accounts ... 410
**Account Database ... 411**
ODBC Selector Wizard ... 412
Creating a New Data Source ... 414
**Windows Address Book ... 418**
**Quotas ... 419**
**Groups ... 420**

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Minger** ... 422
**3 Importing Accounts** ... 423
**Importing Accounts From a Text File** ... 423
**Windows Account Integration** ... 425

## Section VII Lists Menu 430

**1 Mailing Lists** ... 430
**Mailing List Editor** ... 431
Settings ... 431
Members ... 433
Enhanced List Pruning ... 435
Subscription ... 436
Subscribing to Mailing Lists ... 438
Moderation ... 440
Digest ... 441
Routing ... 442
Notifications ... 444
Support Files ... 445
Public Folder ... 447
Active Directory ... 448
ODBC ... 450
Configuring an ODBC Data Source ... 451
Creating a New ODBC Data Source ... 453

## Section VIII Gateways Menu 458

**1 Domain Gateways** ... 458
**Gateway Editor** ... 459
Domain ... 460
Verification ... 461
Configuring Multiple LDAP Verification Queries ... 464
Forwarding ... 465
Dequeuing ... 466
Account ... 468
Quotas ... 469
Options ... 470
**Automatic Gateway Creation** ... 473

## Section IX Catalogs Menu 478

**1 Catalog Editor** ... 478
**2 The PUBLIC Catalog** ... 479

## Section X Queues Menu 482

**1 Mail Queues** ... 482
**Retry Queue** ... 482
**Holding Queue** ... 484
**Custom Queues** ... 486
**Restore Queues** ... 487
**DSN Options** ... 488
**2 Pre/Post Processing** ... 490
**3 Queue and Statistics Manager** ... 491

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Queue Page ... 492
User Page ... 495
Log Page ... 497
Report Page ... 499
Customizing the Queue and Statistic Manager ... 500
MDstats.ini File ... 500
MDStats Command Line Parameters ... 501

Section XI Additional MDaemon Features 504

1 MDaemon and Text Files ... 504
2 Remote Server Control via Email ... 504
Account Access and Control ... 504
Mailing List and Catalog Control ... 506
General Email Controls ... 509
3 The RAW Message Specification ... 509
The RAW Message Specification ... 509
Bypassing the Content Filter ... 510
RAW Headers ... 510
Special fields supported by RAW ... 511
Sample RAW mail messages ... 512
4 Semaphore Files ... 512
5 Message Precedence System ... 518
6 Route Slips ... 518
7 MDaemon and Proxy Servers ... 519

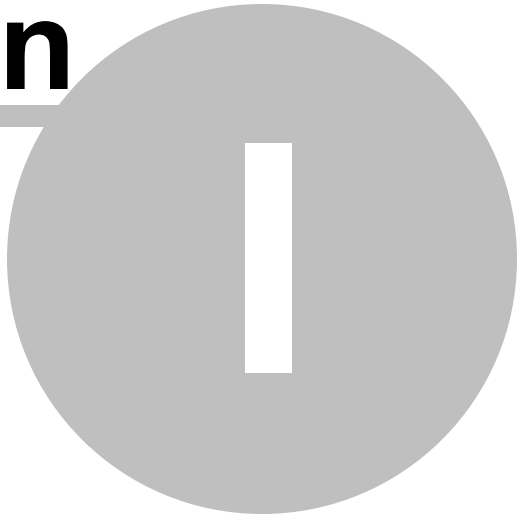
Section XII Glossary 522

Index 543

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section



# 1 MDaemon Messaging Server 13.0

## 1.1 Introduction

### Introduction

Alt-N Technologies' MDaemon Messaging Server v13.0 is a standards-based SMTP/POP3/IMAP mail server that supports Windows 7/Vista/XP/2008/2003 systems and offers a full range of mail server functionality. MDaemon is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. MDaemon offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP and Active Directory support, an integrated browser-based email client, content filtering, spam filters, extensive security features, and more.

### MDaemon Standard and PRO

MDaemon Messaging Server is available in two versions: MDaemon Standard and MDaemon PRO. With the powerful features of MDaemon Standard, you can host your network's email with MDaemon's full-fledged SMTP server, or you can collect your entire domain's email from a single ISP provided POP3 mailbox via the included DomainPOP feature. You can also host multiple Mailing Lists, allow your users to access their email via the included WorldClient webmail component, and utilize a number of other features. MDaemon PRO is equipped with everything in Standard, plus its support for IMAP4, multiple domains, Domain Sharing, Gateways, expanded Mailing Lists, and BlackBerry smartphone integration make it ideal for larger organizations with greater needs. MDaemon PRO also adds group calendar and scheduling, an instant messaging system, multiple language support for WorldClient, automatic domain gateway creation, and more. For a detailed comparison chart outlining the features included in each version, visit: www.altn.com.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## MDaemon Features

MDaemon is equipped with many features besides SMTP, POP3, and IMAP4 email processing. The following is a list of just some of those features.

- MDaemon Pro includes a fully integrated BlackBerry® Enterprise Server, which makes it possible for your users to synchronize their MDaemon email, calendar, contacts, and other PIM data with a BlackBerry device 151.
- Complete support for virus scanning and protection through SecurityPlus for MDaemon. This add-on for MDaemon provides potent anti-virus protection. Messages can be scanned for viruses and cleaned or deleted automatically before ever reaching the intended recipients. Further, you can configure MDaemon to send a message to the administrator, sender, and recipient of the infected message notifying them of the virus. SecurityPlus for MDaemon is a separately licensed product that is available from www.altn.com.
- MDaemon features a complete suite of Mailing List or email group management functions allowing for the formation of an unlimited number of distinct distribution lists that can contain local and/or remote members. Lists can be set to allow or refuse subscription requests, be public or private, post replies to either the list or the originator of the message, be sent in digest format, and be configured using numerous other features.
- An integrated component of MDaemon is WorldClient. This exciting product makes it possible for your users to access their email using their favorite web browser rather than from a workstation dependent email client. This tool is perfect for mobile staff and users who do not have a dedicated machine from which to access their email.
- WorldClient is equipped with a complete suite of email client features. You can: send and receive email, spell check messages, manage your email in multiple personal folders, display the interface in any of 18 languages, schedule meetings and appointments and share calendars and tasks with other users, manage your MDaemon account settings (when used in conjunction with WebAdmin), manage contacts, and more. WorldClient is also equipped with ComAgent, a small utility that can be downloaded and installed on a user's local computer. This provides easy access to your email and folders and checks for new messages without having to open your web browser. It also includes a complete Instant Messaging system that can be used to quickly "chat" with other MDaemon/WorldClient users.
- MDaemon is equipped with many features designed to help you make your email system secure. The Spam Filter and DNS Black Lists features will help you put an end to most "spam" email messages that "spammers" try to route through or to your domain. IP and Host Screening and the Address Blacklist provide the capability to screen and prevent certain addresses and domains from connecting to or sending mail through your system. They also make it possible to connect to specific IP addresses while screening all others.
- Equipped with support for Lightweight Directory Access Protocol (LDAP), MDaemon can keep your LDAP server up to date on all of its user accounts. This makes it possible for you to keep an LDAP address book up to date so that users with email clients that support LDAP can access it. You can also choose to use Active Directory or your LDAP server as the MDaemon account database instead

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

of an ODBC compliant database or the local USERLIST.DAT system. Thus, you can configure multiple MDaemon's at different locations to share the same account database.

- MDaemon's extensive parsing features make it possible to provide email for an entire LAN with as little as a single dial-up ISP POP3 mailbox. This makes it possible to provide email to an entire network for a fraction of the normally associated cost.
- MDaemon can be configured to keep your Windows Address Book or Microsoft Outlook Contact Store up to date with your user information. This provides another means of making a global address book available to your users.
- Address Aliases provides the ability to route email messages addressed to "fictitious" mailboxes to a valid account or mailing list. This makes it possible for individual accounts and lists to have multiple email addresses at one or more domains.
- The Domain Gateways feature provides the option of setting up separate domains for various departments or groups that may be local to your network or located somewhere else on the Internet. Using this feature, all mail addressed to a domain for which MDaemon is acting as a gateway will be placed in that domain's mailbox by MDaemon. It can then be collected by that domain's MDaemon server or email client and distributed to the domain's users. This feature can also be used to enable MDaemon to act as a backup mail server for other domains.
- Accounts can be controlled remotely by users by using specially formatted email messages. This allows greater administrative flexibility, and empowers users by turning day-to-day simple account maintenance tasks, such as changing passwords, over to them.
- Integrated web-based remote administration via WebAdmin. WebAdmin is integrated with MDaemon and WorldClient and enables your users to review and edit their account settings via their web-browser. You can designate which settings that your users may edit, and assign access permissions on a per account basis. WebAdmin can also be used by the Administrator (and whomever else you wish to allow) to review or edit any of MDaemon's settings and any other files that you wish to make available to the WebAdmin system for reviewing.
- With File Catalogs, the email administrator can create password protected groups of files which users can have encoded and automatically sent to them through the use of specially formatted email messages.
- An internal message transport system known as RAW mail provides a simple method for placing messages into the mail stream and greatly simplifies custom mail software development. Using RAW, a complete mail system can be devised using a simple text editor and a couple of batch files.
- A highly versatile Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and more.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### System Requirements

For the most up to date information on MDaemon's system requirements and recommendations, visit the System Requirements page at www.altn.com.

Certain management, security or wireless synchronization features for BlackBerry smartphones may not be available in all markets. Please refer to the features identified in the product release notes or on the MDaemon messaging server website. Certain functionality requires the activation of a BlackBerry smartphone with a compatible data plan. Check with your service provider for availability, costs and restrictions.

Research In Motion (RIM) assumes no obligations or liability and makes no representation, warranty, endorsement or guarantee in relation to any aspect of any third party products or services.

BlackBerry Enterprise Server is not available in some countries and regions.

### Trademarks

Copyright © 1996-2012 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

**See:**

**New in MDaemon 13.0** 15
**Upgrading to MDaemon 13.0** 26
**MDaemon's Main Display** 30
**Getting Help** 22

## 1.2 New in MDaemon 13.0

### New MDaemon Pro Features

#### ActiveSync Device Policy Support 156

MDaemon is now equipped with support for basic ActiveSync device policy. You can

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

view predefined policies and create your own policies from a new screen at: Mobile Device Management » ActiveSync » Policies 156. Policies can be created to require devices to use a password, force passwords to use both letters and numbers, lock devices after a designated number of minutes, and cause the device to be wiped 160 after ten failed password attempts.

A default policy can be assigned per domain from the ActiveSync » Domains 159 screen. Policies can also be assigned per device, from the Account Editor's ActiveSync 355 screen.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies altogether and others may require a device reboot before changes take effect. Further, no policy is applied until the next time the device connects on its own to the ActiveSync server.

## Detect and Stop Hijacked Accounts 306

Dynamic Screening 306 has been improved by adding an option to disable local accounts that try to send more than a specified number of messages in a designated number of minutes. Accounts disabled by this process can still accept incoming mail but they cannot log in to web mail or web administration and they can not collect or send mail. The intent is to try and recognize and stop a hijacked account so that the postmaster can review the situation and take action. Consequently, when an account is disabled a notification email is sent to the postmaster. The postmaster can simply reply to the message to re-enable the account.

## WorldClient Documents Folders 74

The WorldClient themes now support document sharing using document folders. Document folders have full Access Control List (ACL) 79 support like other shared folders 74, which can be used to set permissions and sharing rules, and any types of files can be shared through the system. WorldClient users can upload files to their document folders using the built-in tools. When using the LookOut theme, browsers that support the HTML5 Drag and Drop API, such as Chrome and Firefox, can also upload files by dragging them from the desktop into the browser window. Filenames can be searched and renamed, and files can be attached to new messages that are being composed.

### IMAP "COMPRESS" and "BINARY" Support

The IMAP server now supports the COMPRESS extension (RFC 4978), which compresses all data sent to and from the client. This does require extra memory and CPU usage per IMAP session. You can disable COMPRESS support via a new option at: Default Domain & Servers » Servers 46.

The IMAP server also now supports the BINARY extension (RFC 3516), which lets clients download message attachments in decoded form.

### Simple Message Ticketing System

Public folders 74 can now be configured as a message ticketing public folder through

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the "*Append ticket number to messages sent to this public folder*" option located on the Folder Listing 77 screen. If this is enabled for a public folder MDaemon will add the public folder name and a unique identifier to the subject of messages sent to the submission address of the public folder. Any outbound messages having this specially formatted subject will have the From address changed to the submission address of the public folder and a copy of the outbound message will be placed into a child public folder named "Replied To". In addition, any inbound messages with this specially formatted subject will be automatically redirected to the public folder, regardless of the address the message was sent to.

### ActiveSync Autodiscover Service

MDaemon now supports the ActiveSync Autodiscover Service, which allows users to set up an ActiveSync account with just their email address and password, without needing to know the host name of the ActiveSync server. Autodiscover requires HTTPS 121 to be enabled, and for most systems it also requires that a new CNAME or A-record be added to DNS. "`autodiscover.<your-MDaemon-server>.com`" should resolve to the MDaemon server running ActiveSync (for example, `autodiscover.example.com`).

## Additional Features and Changes

MDaemon 13.0 has many new features and changes. See `RelNotes.html` located in MDaemon's `\Docs\` subfolder for a complete list of all new features, changes, and fixes to MDaemon from the previous version.

---

## New in MDaemon 12.5

### Tablet Support and other WorldClient Improvements

WorldClient's flagship theme, LookOut, has undergone major architectural and design changes to accommodate tablet devices such as the BlackBerry PlayBook and the iPad. Users should not have to change any settings to take advantage of these changes. These changes include:

- Single finger scrolling.
- Dragging and dropping between folders with one finger; use two fingers to copy to the destination folder.
- No popup windows for message composition, item entry and item editing to help maintain context.
- Inline message preview to help preserve the flow of the mail folder and maximize screen real estate.

### Other WorldClient improvements

- ComAgent chatting has been moved to a side panel instead of being in a 'floating' tab that may cover other parts of the interface (Lookout theme).
- Calendars can now be viewed together to help see schedules for multiple users (Lookout theme).
- Autoresponder settings moved to their own page under Option to help make

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

management easier.

- Various HTML5 & CSS3 features have been used to improve performance and loading time (Lookout theme). The Compose page now uses app-caching to help load the HTML editor more quickly (particularly over SSL connections) on browsers such as the PlayBook, Chrome and Firefox that support the manifest HTML attribute.
- Advanced message searching has now been enhanced with a number of other new search parameters to help make finding messages easier.
- WorldClient's LookOut theme now auto-saves draft messages every minute.

## ActiveSync for MDaemon Improvements 154

ActiveSync for MDaemon has been improved and is now capable of synchronizing email as well as personal information manager (PIM) data. For information on configuring your specific ActiveSync device see the documentation that accompanied your device. Some information on basic device configuration is available from the Alt-N Technologies website: Windows Mobile, iOS, and Android.

ActiveSync for MDaemon is a separately licensed product available from Alt-N Technologies. ActiveSync for MDaemon will not work beyond a one-time 60-day evaluation period unless a license is purchased.

### Spam Filter Updated to Include SpamAssassin 3.3.2

MDaemon's Spam Filter 241 has been updated and now includes SpamAssassin 3.3.2. A summary of changes and other documentation on SpamAssassin can be found at the SpamAssassin website.

The Spam Filter updates 260 option: *Run SA-UPDATE as part of update process* has been removed. This will now always take place. The old and out-dated method based on `UpdateSpamAssassin.exe` has been removed and that file has been deleted. MDaemon now relies on sa-update to perform all necessary SpamAssassin updates. Also, the `80_MDaemon_updates.cf` file is no longer used and has been deleted.

Finally, the installer was changed to no longer delete existing `.cf` rule content. The rule updating process will manage `.cf` files.

## BlackBerry® Mobile Data System Connection Service (MDS-CS) 175

MDaemon's BlackBerry Enterprise Server (BES) now includes MDS-CS 175. MDS-CS permits behind-the-firewall access to files and web applications from BlackBerry devices. It receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, and sends login requests so that users can view Internet and Intranet content on their BlackBerry devices. This will, for example, allow you to access your private Intranet without a VPN connection.

You can find more information about MDS-CS at BlackBerry.com, but please note that not all of the features and capabilities documented there are supported by MDaemon.

### Global Recipient (RCPT) Blacklist

Located under `Security » Security Settings... » Screening`, the Address Blacklist

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

screen has been renamed to Sender Blacklist 299 and a new Recipient Blacklist 301 feature has been added. The new Recipient Blacklist operates on SMTP envelope RCPT data only (not message headers). Also, the `Blacklist.dat` file has been renamed `SenderBlacklist.dat` and a new `RecipientBlacklist.dat` file has been created. The `BLACKLIST.SEM` Semaphore File 512 reloads both files into memory.

### Personal Sender (MAIL) Blacklist

Each account now has a personal Blacklist contact folder. Incoming messages from any SMTP mail sender listed in the Blacklist will be rejected with "`550 recipient unknown` ." Messages that make it past SMTP and into the local queue but have a blacklisted address in the `From:` or `Sender:` header will be moved to the bad message folder. The Blacklist folder is automatically created the next time a message is received for the account. Users can manage their account's Blacklist folder via WorldClient just as with the Whitelist folder.

### Outbound Message Sending Quotas

New quota options are available in the New Account Defaults 385 and Account Editor 366 which let you set a limit to the number of messages an account can send via SMTP per day. The counter automatically resets to zero for all accounts at midnight each night. Note that it is possible to exceed this limit slightly if messages come in faster than the cache can keep up.

## Improved Use of DNS 51

When MDaemon is configured to use Windows DNS servers it will now use all servers found instead of just the first two. This required several internal changes including doing away with the old "max retry attempts" option for DNS lookups. MDaemon will now try each DNS server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. Also, on startup, the System log will display each DNS server that MDaemon will use and an indicate where it came from (i.e. manually configured or taken from Windows). Further, the options for designating a primary and secondary DNS server have been removed. Now there is just a single edit box that lets you manually configure as many DNS servers as you want. Finally, the options to use Windows DNS servers or manually configured DNS servers are no longer mutually exclusive. If you configure both, MDaemon will use both.

### Configuration Session Improvements

The Configuration Session interface has been improved in several ways. For example, the right-click menu now works properly and allows you to disconnect an active session and you can double-click or view Properties of one or more active sessions, which displays the session log. You can also submit the connecting IP address to the IP and/or Dynamic Screen features. Also, the Sessions Window 36 will update individual line items more efficiently and handle a much larger amount of session data. Further, Configuration Sessions can now change the primary domain name. Finally, changes made to the IP Screen, Host Screen, and Address Blacklist via WebAdmin will now be picked up by configuration sessions.

## Improved IP Shield Protection 273

There are several improvements to the IP Shield 273:

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

- The IP Shield now has a master on/off switch. It is enabled by default but will have no effect when there are not yet any configured domain/IP pairs.
- It supports the `$LOCALDOMAIN$` macro which expands to cover all local domains (including gateways). If you use this macro it is no longer necessary to keep the IP Shield up to date when local domains or gateways change. Existing installations will not have their existing IP Shield values altered in any way. However, there is a new *Default* button that can be used to convert existing IP Shield values to the new `$LOCALDOMAIN$` system. By default, entries are added to the IP Shield associating all reserved IP address ranges with `$LOCALDOMAIN$`.
- When the *Don't apply IP Shield to authenticated sessions* option is enabled, the IP Shield restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be "Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message.
- Also, the IP Shield has a new option that is disabled by default: *Check FROM header address against IP Shield*. If you enable this option then the IP Shield will compare the address taken from the message's `FROM` header in addition to that taken from the `SMTP MAIL` value. Note that this option can lead to problems with incoming list messages and other types of messages. It should not be enabled unless you are sure you need it.
- The `IPShield.dat` file is now cached in memory to increase access speed. Create an `IPSHIELD.SEM` to reload the file into memory.

---

## New in MDaemon 12

### BlackBerry Enterprise Server 162

MDaemon Pro is equipped with a BlackBerry Enterprise Server, which makes it possible for your users to synchronize their MDaemon/WorldClient email, calendar, and other personal information management (PIM) data with their BlackBerry smartphones. BlackBerry platform support also makes it possible for you to set security polices for user devices and even erase a device should it be lost or stolen.

MDaemon's BlackBerry Enterprise Server features include:

- No need for third-party sync clients. Each user's data is synchronized using software already present on all BlackBerry devices.
- MDaemon/WorldClient email (including mail folders) is synchronized with the device in both directions. Therefore whether mail is read, moved, deleted, etc. on the device or the server it will be synchronized on both.
- Two-way Calendar synchronization. For example, if you create a new appointment, set a reminder, or modify an appointment on either the device or within WorldClient it will be synchronized in both places.
- Two-way tasks and notes synchronization.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

- Global address book lookup.
- Scheduling with free/busy.
- Limited BlackBerry device policy support, so that you can set device policies such as: require passwords, expiring passwords, encrypt media files, and more.
- Set different policies for individual domains or users.
- Remotely change the device's password and lock it.
- Erase all data from the device, for example if it is lost or stolen.
- Backup and Restore options for your BlackBerry Enterprise Server database.

MDaemon's main BlackBerry Enterprise Server options are located at: Setup » BlackBerry... » BlackBerry Enterprise Server 162, and the account specific options are located on the BlackBerry Enterprise Server 351 screen of the Account Editor.

## ActiveSync for MDaemon 154

MDaemon includes support for "ActiveSync for MDaemon," which is a separately licensed OTA ActiveSync (AirSync) server. This server is capable of synchronizing a user's default calendar and default contact data between his MDaemon/WorldClient account and an ActiveSync capable device. MDaemon's ActiveSync options are located under: Setup » Web, Sync, & IM Services... » ActiveSync 154, and there is an option on the Account Editor's Options 377 screen if you wish to disable it for certain users. The ActiveSync screen contains options for enabling or disabling it for individual domains, setting the session timeout value, and designating the level of detail for the ActiveSync logs. There are also links to instructions on how to configure devices to use ActiveSync.

When you enable ActiveSync for MDaemon the first time it will operate for 60 days on a trial basis so that you can see if you like it. After that there is a one-time license fee if you wish to continue using it. You can acquire a license key from www.altn.com or your local distributor/reseller.

## WorldClient Improvements

- ComAgent chat is now included in the LookOut theme. When this feature is enabled from a new option on the Personalize page in WorldClient, a ComAgent bar will appear in the lower right corner of the browser. This allows users to view their buddy list and chat with their ComAgent buddies just as when using the ComAgent application.
- Updated WYSIWYG editor. This should deliver improved performance for message compose load times, and it includes improvements and fixes in both message generation and composition.
- The calendar views in WorldClient's LookOut theme were redesigned to allow for enhanced event rendering and to give a more desktop-like experience.
- You can now edit a single occurrence of a recurring event within WorldClient's calendar.
- The desktop themes can now have a To column. When enabled, this will cause

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the Sender column to always display the From field. Previously the From column would change between To and From depending on whether the user was in the Sent Items folder or not. Users can enable this column from Options » Columns in WorldClient.

**See:**

**Introduction** 12
**Upgrading to MDaemon 13.0** 26
**MDaemon's Main Display** 30

## 1.3 Getting Help

### Support Options

Support is a vital part of the total Alt-N Technologies customer experience. We want you to get the most from our products long after the initial purchase and installation and we are dedicated to ensuring that any issues are resolved to your satisfaction. For the latest Customer Service information, Technical Support Options, Self-support Resources, Product Information, and more, visit the Alt-N Technologies support page at: www.altn.com/support/

### MDaemon Beta Testing

Alt-N Technologies maintains active beta testing teams for our products. If you would like information about joining the MDaemon beta team, send a message to MDaemonBeta@altn.com.

The Beta Team is for those who wish to acquire Alt-N software before its general release and aid in its testing; it is not a technical support alternative. Technical support for MDaemon will only be provided through those methods outlined at: www.altn.com/support/.

### Contact Us

**Hours of Operation**
M-F 8:30 am - 5:30 pm Central Standard Time
Excludes weekends and U.S. holidays
Customer Service or Sales
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
sales@helpdesk.altn.com

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Technical Support**
www.altn.com/support/

**Training**
training@altn.com

**Business Development/Alliances**
alliance@altn.com

**Media/Analysts**
press@altn.com

**Channel/Reseller Inquiries**
Please refer to the Channel Partner page for additional information.

## Corporate Headquarters

**Alt-N Technologies, Ltd.**
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
Fax: 817-601-3223

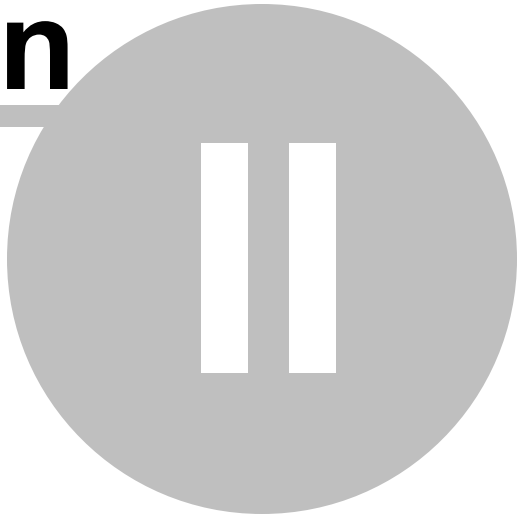
## Trademarks

Copyright © 1996-2012 Alt-N Technologies, Ltd. Alt-N®, MDaemon®, and RelayFax® are trademarks of Alt-N Technologies, Ltd.

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, BBM™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license. Apple is a trademark of Apple Inc. Windows Mobile, Microsoft and Outlook are trademarks of Microsoft Corporation. Palm is a trademark of Palm Trademark Holding Company, LLC. All other trademarks are the property of their respective owners.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section



# 2 Upgrading to MDaemon 13.0

Below is a list of special considerations and notes that you may need to be aware of when upgrading to MDaemon version 13.0 from a previous version.

## Version 13.0.0

- MDaemon FREE is no longer supported and the FREE registration key will not work beginning with this version. The last MDaemon FREE version is MDaemon 12.5. The MDaemon installation process will offer to convert FREE installs to TRIAL installs.
- A new global on/off setting was added for SyncML 191 and ActiveSync 154 servers to enable/disable them globally for all domains. Please check to be sure the SyncML and ActiveSync servers are enabled/disabled per your liking. This global switch is now used for ActiveSync when enabling/disabling it via the FILE menu and "Servers" section of the main UI.
- MDaemon no longer checks messages for RFC compliance by default to avoid an issue with Outlook's test messages (which are missing the Date header). Check Default Domain & Servers » Servers 46 to make sure the *...refuse messages which are not RFC compliant* setting is how you like it.
- MDaemon no longer supports Windows XP older than Service Pack 2 or Windows Server 2003 older than Service Pack 1.

## Version 12.5.0

- The ActiveSync for MDaemon license key is now subject to product activation. Trial keys must be activated within 5 days and production keys within 30 days. For more information on product activation, see: Product Activation Frequently Asked Questions at altn.com.
- Incorporation of MDS-CS 175 has required that your *BlackBerry Enterprise Server logging* value found at Setup » BlackBerry... » Options 179 be reset to a default value of "Informational". If this is not your desired setting you can change it there.
- The Domain Sharing 64 option *Incoming Minger lookups trigger Domain Sharing processing* has been removed. If you have multiple servers using Domain Sharing and you are careful to configure each node to use all the other nodes for Domain Sharing (if appropriate for your setup), then this option should not be needed.
- The *Over quota accounts can accept mail but not send mail* option (located at Accounts » Account Settings » Quotas 419) has been removed and replaced with two separate options: *Refuse incoming messages sent to over quota accounts* (enabled by default) and *Refuse outgoing messages sent from over quota accounts* (disabled by default). These new defaults may not replicate previously configured behavior so check and change as needed.

## Version 12.0.0

- Windows 2000 is no longer a supported operating system. MDaemon 12.0

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

requires Windows 2008, 2003, 7, XP, or Vista.

- WorldClient has an updated version of the CKEditor WYSIWYG editor for message composition. If you do not have custom themes it is recommended that you remove the `MDaemon\WorldClient\HTML\fckeditor\` directory. This directory is not removed by the installer because of template customization.
- MDaemon's new BlackBerry Enterprise Server (BES) 162 feature could result in duplication of data when combined with other sync techniques like SyncML or BlackBerry Internet Service 183 Integration. Care must be taken to avoid this (see BlackBerry Device Activation 164).
- Passwords must now be at least 4 characters long. Existing passwords are not forced to change, but the next time you do change one the new password must have at least 4 characters.

## Version 11.0.0

- MDaemon's POP and IMAP servers now require use of the full email address as the user name/login credential. If a user's mail client is configured to use only the mailbox value as the login (for example, "user1" instead of "user1@example.com"), he will not be able to log in to MDaemon using that client until he changes the client's configuration to use the full email address instead. If you wish to continue to allow mailbox only logins then you can disable the option, "*Servers require full email address for authentication*," located on the System 195 screen under Preferences. We strongly recommend that you leave this option enabled, requiring full email addresses.
- Attachment Linking 142 has undergone a complete overhaul and as a result its configuration has been reset to the default value. When upgrading to MDaemon version 11.0, all accounts currently configured to use Attachment Linking will be set to extract attachments to the FILES folder. You may therefore need to manually reconfigure accounts that you wish to use Attachment Linking.
- The `WorldClient.dll` was updated to dynamically generate the `robots.txt` file in the WorldClient HTML directory to be explicit about which files should not be indexed. If you wish to disable this behavior then edit the `WorldClient.ini` file and set the value: `ModifyRobotsTxt=No` under the `[WebServer]` section. Alternatively if the `robots.txt` file is read-only it will not be touched. Further, custom `Logon.html` files need to have the following meta tag inserted into their headers: `<meta name="ROBOTS" content="NOINDEX, FOLLOW">`.
- The Globe and Redline themes within WorldClient were discontinued and are no longer supported. When you run MDaemon 11.0 for the first time it will move the \Templates\ and \HTML\ folders for these two themes to \WorldClient\Old\. They can be safely deleted if you decide not to manually maintain these themes yourself.
- *Check a DKIM DNS Record*, located at http://dkimcore.org/tools/dkimrecordcheck.html, is a tool for checking your DKIM DNS setup for compliance with the DKIM specification as published in RFC 4871. Given a selector and a domain this tool will retrieve the DKIM key record from DNS, parse it using the BNF from the DKIM specification, and then sanity check the various fields. In the end you'll get a good/bad result letting you know whether your DKIM DNS setup is "to spec" or not. Note: this site is a work in progress and is not hosted or

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

created by Alt-N Technologies.

- The default options for quota calculations have been reset. Review your settings on the Quotas 419 screen to make sure they are as you desire. The default for including Inbox sub-folders when calculating quotas has been changed from FALSE to TRUE.
- As part of the new BlackBerry Internet Service (BIS) 183 integration feature, MDaemon requires all IMAP/POP sessions from BlackBerry Internet Service users to use a full email address when logging in to MDaemon. Thus when configuring their BlackBerry devices to collect mail they will need to use the full email address as the login parameter instead of just the mailbox portion of the address. This is necessary in order to avoid possible conflicts and to achieve proper account integration. This might mean that some of your existing users will have to delete and recreate the mail profile on their device, or at least change their login value to the full address.
- See `Relnotes.html` located in MDaemon's `\Docs\` sub-folder for a complete list of all new features, changes, and fixes to MDaemon from the previous version.

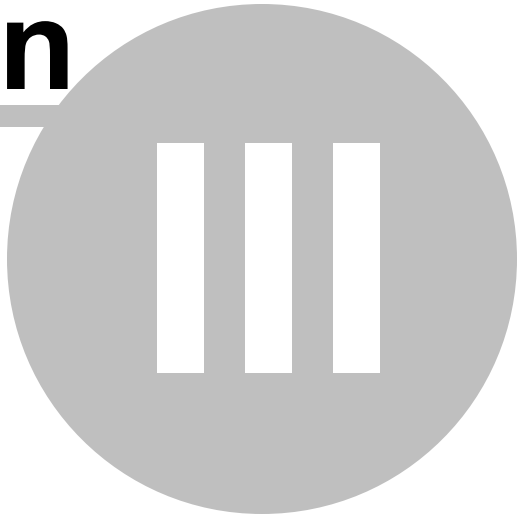
---

**See:**

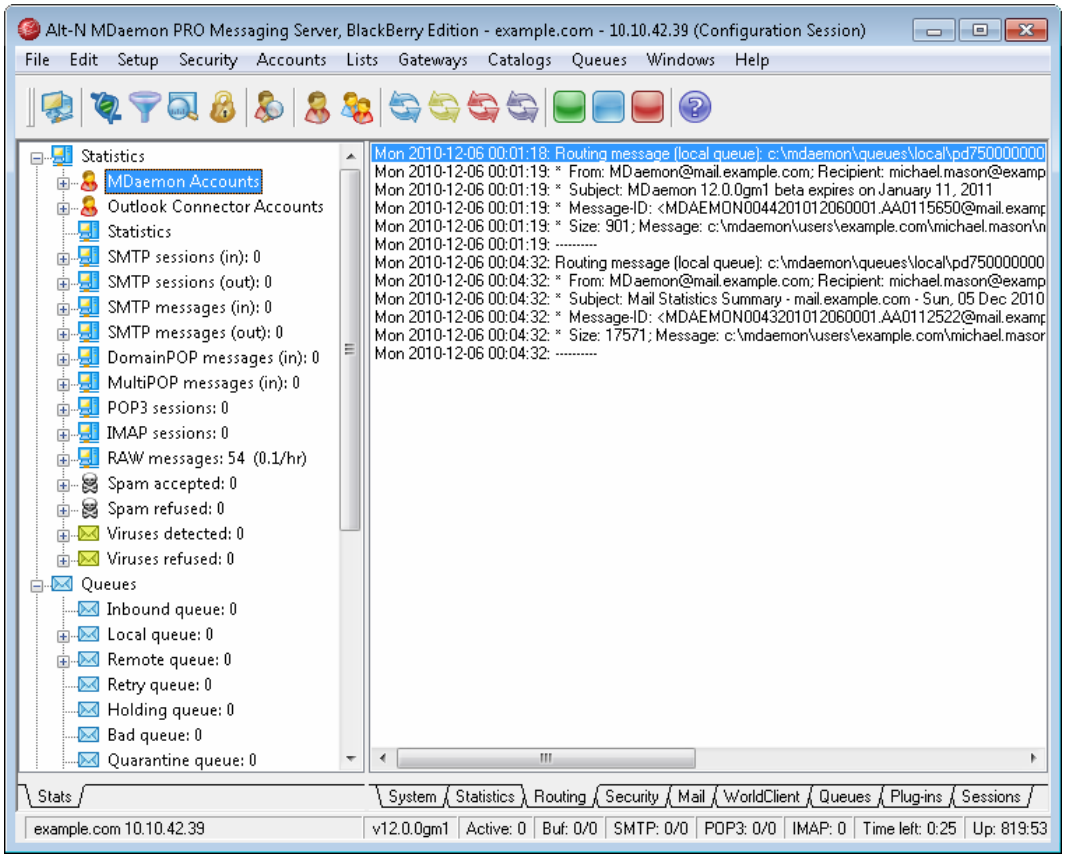
**Introduction** 12
**New in MDaemon 13.0** 15
**MDaemon's Main Display** 30

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section



# 3 MDaemon's Main Display




MDaemon's main graphical user interface (GUI) gives you important information regarding MDaemon's resources, statistics, active sessions, and queued mail waiting to be processed. It also contains options for easily activating/deactivating MDaemon's various servers. The GUI's tabbed panes keep you up to date on how the server and its incoming and outgoing connections are performing.

## Stats

The Stats pane is the default left pane of MDaemon's main interface. This pane contains three sections: Statistics, Queues, and Servers.

The *Statistics* section contains statistics regarding the number of messages sent and received by MDaemon as well as the number of POP3 and IMAP sessions that have been initiated since startup. This section also tells you how many user accounts exist and how many more can be created. Statistics contains two right-click shortcut menus: one for the accounts items and one for the mail counter statistics items. The accounts shortcut menu provides shortcuts for creating, editing, and deleting accounts. The mail counter statistics items have a shortcut menu that can be used to clear the counts.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

When you click the "reset root node counters" option, all of the counters will be reset, not merely the one you right-click. Further, there is an option at Setup » Preferences » GUI that can be used to "*Preserve root node mail counters across reboots*." Otherwise they will be reset whenever the server is rebooted.

The *Queues* section contains an entry for each message queue and the number of messages (if any) that each queue contains. You can right-click on each of the queue entries to open a shortcut menu containing one or more of the following options, depending on which queue you select:

**View Queue** — this option switches the main pane to the Queues tab and displays the selected queue. A list of all messages the queue contains will be displayed, and you can right-click any message to open a shortcut menu containing numerous options similar to those available in the Queue & Statistics Manager such as Copy, Move, Edit, White list, and so on.

**Queue and statistics manager** — open the Queue and Statistics Manager to the Queue Page with the selected queue displayed.

**Process Now** — this option "re-queues" all messages contained in the queue and attempts to process them normally for delivery. If you attempt to process messages contained in the Holding queue, Bad queue, or the like then the messages may encounter the same errors that put them there in the first place and return them to the same queue.

**Freeze/unfreeze queue** — temporarily pauses processing for the selected queue, or continues the processing if it is currently paused.

**Release** — releases messages from the Holding Queue. MDaemon will attempt to deliver the messages regardless of errors encountered — they will not be returned to the Holding Queue even if they encounter the same errors that caused them to be moved there originally.

**Re-Queue** — This is available for the Holding Queue, and has the same effect as *Process Now* above.

**Enable/disable queue** — activates or deactivates the Holding Queue. When disabled, messages will not be moved to the Holding Queue regardless of errors encountered.

The *Servers* section contains an entry for each server within MDaemon, and each entry lists the current state of the server: "Active" or "Inactive". Listed below each server's entry is an entry for each domain (when applicable) and the port and IP address currently in use by that server or domain. The shortcut menu provides a control for toggling each server between the Active and Inactive state. When a server is inactive its icon will turn red.

## Event Tracking and Logging

The default right-hand pane of the main interface contains a group of tabs that display MDaemon's current actions and the status of its various servers and resources, and they are continually updated to reflect current server conditions. Each active session

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

and server action is logged onto the appropriate tab once each action is complete. The information displayed on these tabs is mirrored in the log files kept in the Logs directory, if you have chosen to log such activity.

The primary pane of MDaemon's GUI contains the following tabs:

**System** — at program startup, the System tab displays a log of the Initialization Process, which can alert you to possible problems with MDaemon's configuration or status. It also displays activity such as enabling/disabling any of MDaemon's various servers.

**Statistics** — this tab will display a server statistics report corresponding to the information contain in the various root node counters on the Stats tab in the Stats and Tools pane. If you wish to change the font or font size used for this report you can do so by editing the following keys in the MDaemon.ini file:

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

Further, at midnight each night, the Postmaster and all addresses listed on the Recipients 227 screen of the Content Filter will get a copy of this report via email. This is the same report that is generated when you use the "Status" email command listed in the Remote Server Control via Email section. If you do not wish this report to be sent, then disable the "*Send stats report to postmaster at midnight*" option located on the Miscellaneous 202 screen under Preferences.

**Routing** — displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

**Security** — click this tab and several other security-related tabs will appear above it.

**Content Filter** — MDaemon's Content Filter 212 operations are listed on this tab. When a message matches the criteria of one of the Content Filter's message rules, the relevant information related to that message and the actions taken are logged here.

**AntiVirus** — if you have installed SecurityPlus for MDaemon 210, then all AntiVirus operations are listed on this tab. When a message is scanned for viruses the relevant information related to that message and the action taken is logged here.

**AntiSpam** — displays all of MDaemon's spam filtering 241 and prevention activities.

**MDSpamD** — lists all activity of the MDaemon Spam Daemon 251.

**SPF/Sender ID** — displays all Sender Policy Framework and Sender ID 282 activities.

**DK/DKIM** — lists all DomainKeys and DomainKeys Identified Mail 284 activities.

**VBR Certification** — this tab displays VBR Certification 294 activities.

**Screening** — this tab displays Tarpitting 328 and Dynamic Screening 306 activities.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Mail** — click this tab and several other mail-related tabs will appear above it.

**SMTP (in)** — all incoming session activity using the SMTP protocol is displayed on this tab.

**SMTP (out)** — all outgoing session activity using the SMTP protocol is displayed on this tab.

**IMAP** — mail sessions using the IMAP protocol are logged on this tab.

**POP3** — when users collect email from MDaemon using the POP3 protocol, that activity is logged here.

**MultiPOP** — this tab displays MDaemon's MultiPOP mail collection activities.

**DomainPOP** — this tab displays MDaemon's DomainPOP activity.

**LDAP** — displays LDAP server activity.

**Minger** — displays Minger 422 server activity.

**RAW** — RAW or system generated message activity is logged on this tab.

**Outlook Connector** — displays all Outlook Connector activities.

**BES** — displays activities related to MDaemon's BlackBerry Enterprise Server 162 support.

**BIS** — displays activities related to MDaemon's BlackBerry Internet Service 185 support.

**WorldClient**

**WorldClient** — displays WorldClient's mail activities.

**SyncML** — this tab mirrors the data contained in the SyncML log file.

**Queues** — this tab gives access to another row of tabs above it with one tab corresponding to each message queue, such as: Local, Remote, Holding, Quarantine, Bayesian Spam, and so on.

**Plug-ins** — displays all activities related to any MDaemon plug-ins.

**Active Directory** — displays all Active Directory related activity.

**Sessions** — click this tab and several other tabs will appear above it. These tabs display an entry for each active connection to MDaemon. Whether the connection is SMTP in or out, POP in or out, IMAP, WorldClient, or some other type, information about each active session is displayed here. Double-click on an active session to display a Session Window 36, which displays the transcript of the SMTP session as it progresses.

The information displayed on these tabs has no affect on the amount of data that is actually stored in the log files. However, MDaemon does support a great deal of flexibility with regard to the amount and type of information that is logged in those files. See the Logging 99 dialog for more information on logging options.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Event Tracking Window's Shortcut Menu

If you right-click in any of the Event Tracking pane's tabs it will open a shortcut menu. Various options are provided on this menu that can be used to select, copy, delete, or save the contents of a given tab. The menu's *Print/Copy* option will open any currently selected text in Notepad, which can then be used to print the data or save it to a file. The *Delete* option will delete the text you have selected. The *Search* option will open a window in which you can specify a word or phrase to search for in the log files. MDaemon will search all log files for the text string and then all session transcripts containing that string will be combined into a single file and opened in Notepad for your review. A practical use of this feature would be to search for a particular Message-ID, which would provide a compilation from all the logs of all session transcripts containing that Message-ID.

The layout of the MDaemon GUI is not limited to the default positions described above. You may switch their position by clicking Windows » Switch Panes on the menu bar.

## Composite Log View

Located on the Windows menu of MDaemon's menu bar is the Composite Log View option. Clicking this option will add a window to the GUI that will combine the information displayed on one or more of the main pane's tabs. Use the options on the Composite Log 101 screen of the Logging dialog to designate the information that will appear in that window.

**See:**

**Session Window** 36
**Tray Icon** 34
**Shortcut Menu** 35
**Composite Log** 101

# 3.4 Tray Icon

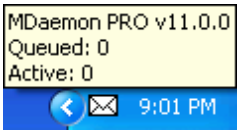
Whenever the MDaemon server is running, its icon will be visible in the system tray. However, apart from simply letting you know whether the server is running, the icon is also dynamic and will change colors based upon the current server status. The following is a list of the icon indicators:

| | |
|---|---|
| | All okay. No mail in local or remote queues. |
| | All okay. Mail in local or remote queues. |

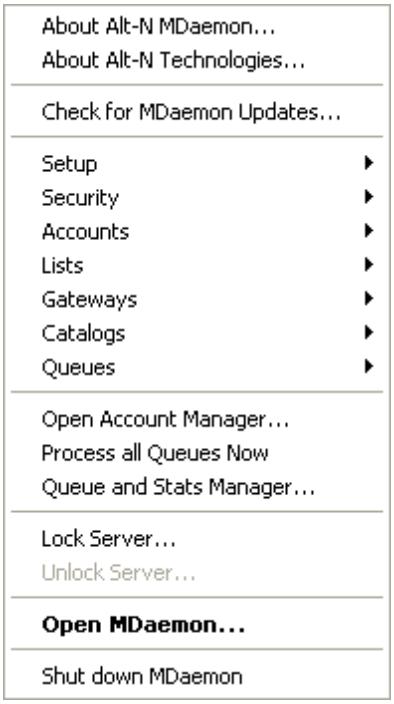
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| | Available disk space below threshold (see Setup » Preferences » Disk[197]). |
| | Network is down, dialup failed, or disk is full. |
| Icon Blinking | A newer version of MDaemon is available. |

There is additional information about the server available through the icon's tool tip. Pause the mouse pointer over it and the tool tip will appear, displaying the number of currently queued messages and active session.




## Shortcut Menu




Right click on MDaemon's tray icon to open the shortcut menu. This menu gives you quick access to virtually all of MDaemon's menus without having to open the main user interface.

Click the "About Alt-N..." options in the top section of the shortcut menu to find out more about MDaemon or Alt-N Technologies.

In the next section, click "Check for MDaemon Updates..." to see if there is a newer version of MDaemon available for download.

In the third section you can access the following MDaemon menus: Setup, Security, Accounts, Lists, Gateways, Catalogs, and Queues. Each of these cascading menus is identical to the menu of the same name located on the menu bar of the main interface.

The fourth section has options to open the Account Manager and Queue and Statistics manager, and one that will cause all of MDaemon's mail queues to be processed.

Next, there are commands to lock and unlock MDaemon's interface (See "Locking/Unlocking MDaemon's Main Interface" below) followed by the "Open MDaemon..." menu selection, used

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

for opening/restoring MDaemon's interface when it is minimized to the system tray.

The last option is "Shut down MDaemon," which is used to quit MDaemon or shut down its system service (the service settings are not changed—the MDaemon service is merely stopped).

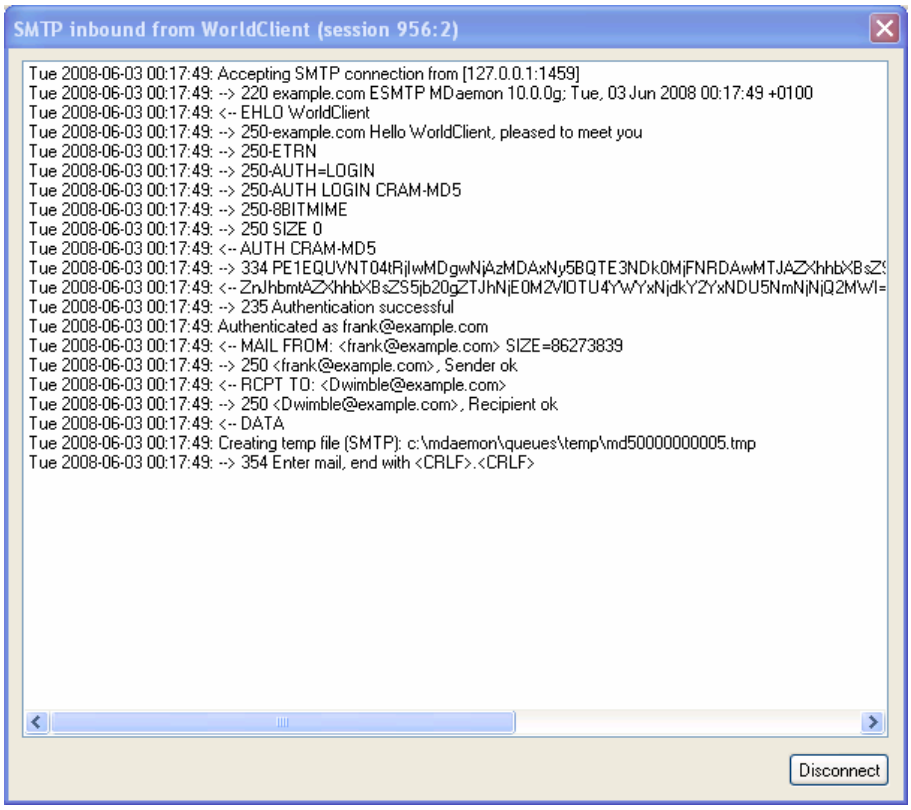
### Locking/Unlocking MDaemon's Main Interface

To lock the user interface, minimize MDaemon, click the "Lock server..." menu item and then enter a password into the box that opens. After confirming the password by entering it a second time, MDaemon's user interface will be locked. It cannot be opened or viewed, but MDaemon will continue to function normally. You will, however, still be able to use the "Process all queues now..." shortcut option to process the mail queues manually. To unlock MDaemon, open the "Unlock MDaemon" dialog by double-clicking the tray icon, or by right-clicking the icon and then choosing "Unlock Server..." Then, enter the password that you created when you locked it.

## 3.5 Session Window

When you double-click an active session on one of the Session tabs[31] of the main GUI, this will open the session window corresponding to that entry. The session window will display the SMTP transcript of that session as it progresses. You can click Disconnect on this window if you wish to interrupt and disconnect that session in progress.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

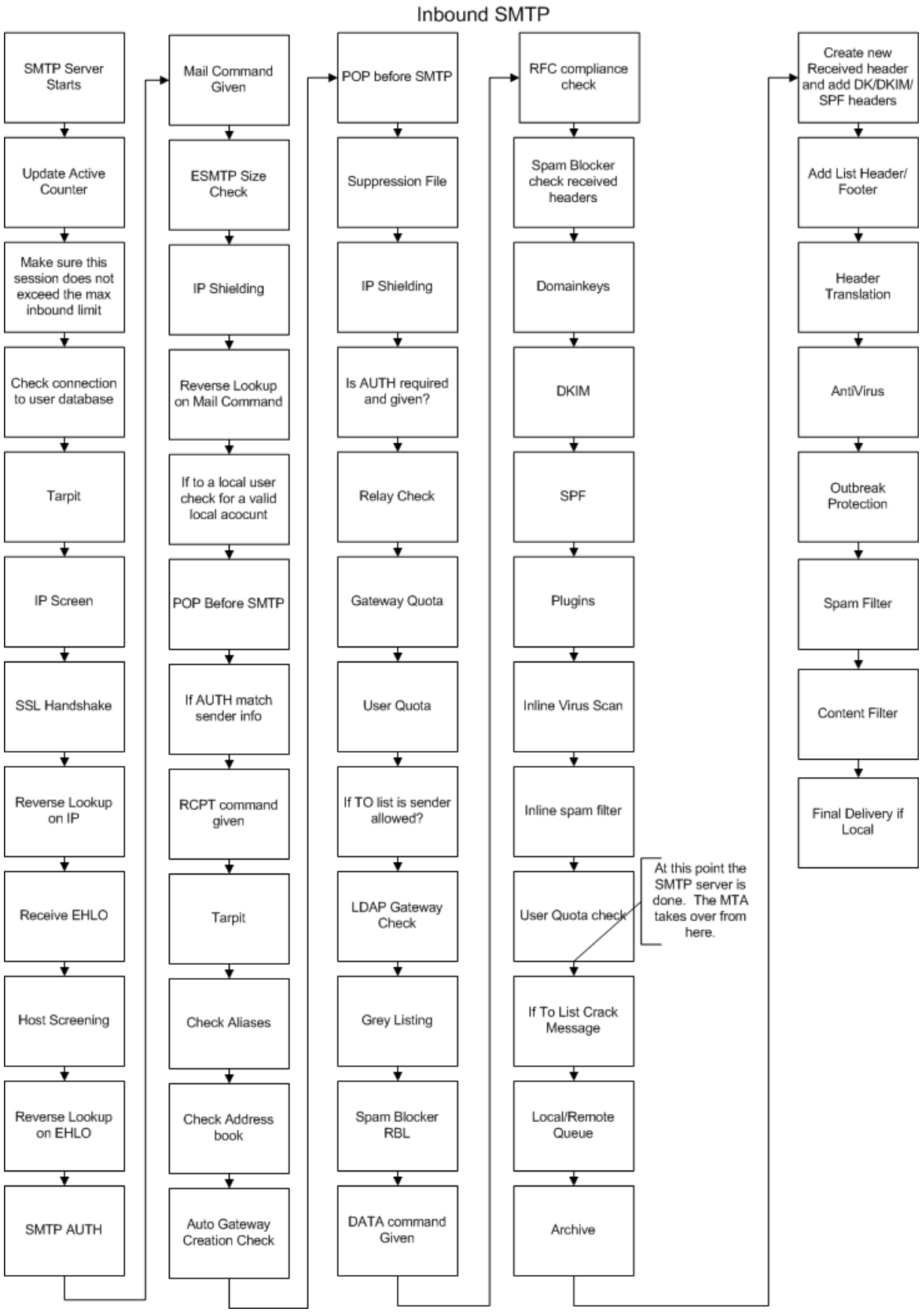



## 3.6 MDaemon's SMTP Work Flow

When an incoming SMTP connection is made, MDaemon goes through a complex series of processing steps to determine whether to accept the message for delivery, and what to do with it once it is accepted. The following chart is a graphical representation of this work flow for inbound SMTP messages.

The extent to which these steps are executed is dependent upon your particular configuration. One or more steps might be skipped if a given feature is disabled in your configuration.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# Section

# 4 Setup Menu

## 4.1 Default Domain / Servers

### 4.1.1 Default Domain & Servers

The Default Domain & Servers section can be reached via the Setup » Default Domain/ Servers... menu selection and is used to configure your default domain and other server options. Only one default domain can be configured, but MDaemon can manage mail for any number of other domains 108 (MDaemon PRO only), and store mail for Domain Gateways 458 as well.

The Default Domain section contains the following dialogs, which are necessary for configuring MDaemon.

**Domain** 41
This screen contains your default domain's name and IP address.

**Delivery** 43
Here you will specify the degree to which you want MDaemon itself to handle delivery of mail versus relaying it to an ISP, gateway host, or other server for it to deliver the mail for you.

**Servers** 46
This screen is used for configuring a number of server and email protocol related options. For example, there are options for choosing whether or not MDaemon's SMTP server will honor VRFY, EXPN, APOP and CRAM-MD5, and more. You can also set a message size limit, limit the number of RCPT statements allowed during the SMTP session, and configure a number of other options.

**Ports** 49
This screen contains the ports that MDaemon will monitor and use for SMTP and POP email delivery. You can also designate the port on which MDaemon will listen for IMAP events, the UDP port used for querying DNS servers, and a number of other port settings. In most cases the default settings will not need to be changed. However, being able to change your port settings is useful when attempting to integrate MDaemon with various other components or servers that you may be using on your network.

**DNS** 51
This dialog is used for designating your primary and backup DNS server IP addresses. It also contains various options governing MDaemon's handling of MX records.

**Timeouts** 55
This area contains various time limits that MDaemon will observe while connecting to remote hosts, waiting for protocol dialogs, waiting for DNS server responses, and so on. In addition, this dialog contains the *Maximum message hop count* limit, which is used to help prevent messages from being caught in a delivery loop.

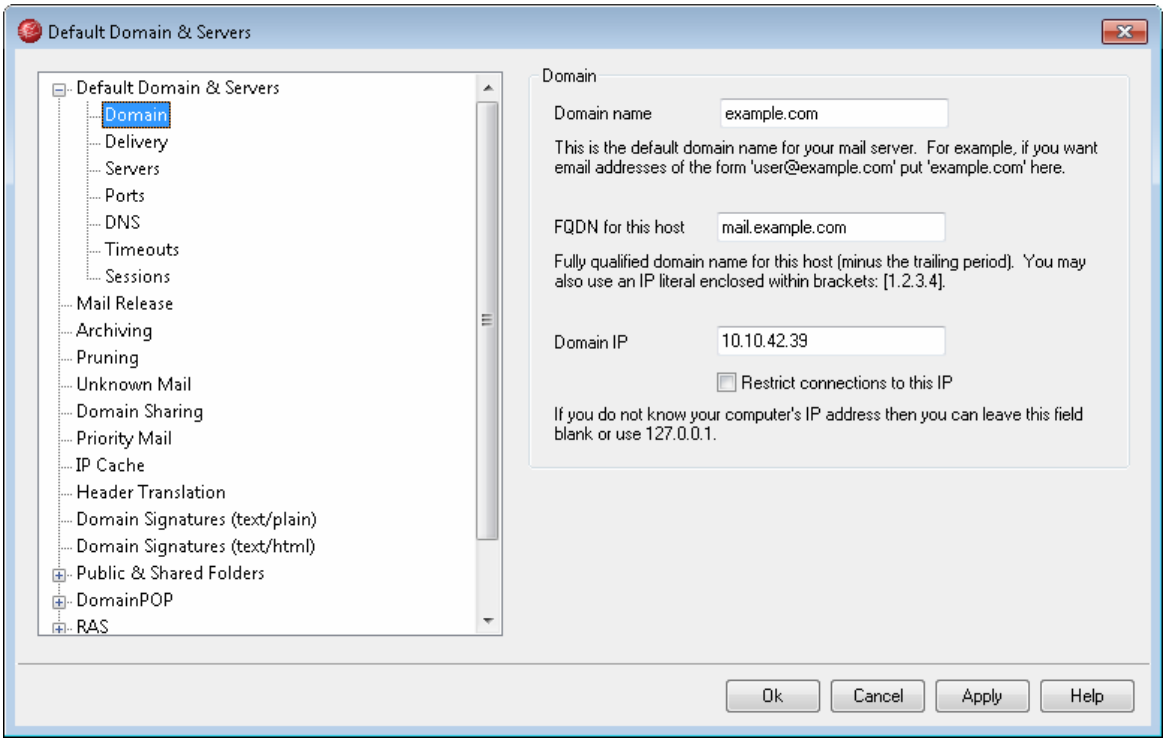
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Sessions** 55
Here you will designate the maximum number of concurrent session threads that MDaemon will use for sending and receiving SMTP, POP, and IMAP mail. You will also designate the number of messages that MDaemon will attempt to send or receive at the same time. In addition you can set a limit on the number of outbound SMTP messages that will be spooled per session thread.

**See:**

**Domain Manager** 108
**Gateway Domains** 458
**DomainPOP Mail Collection** 81

### 4.1.1.1 Domain




**Domain**

**Domain name**
Enter your Default Domain name here. This is the default domain name used when creating new accounts. It is also used in the WorldClient accounts that are created automatically when you are utilizing the MDaemon/WorldClient Integration features. Typically, the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Alternatively, you may choose to use an internal-only or otherwise non-valid, non-public domain name (such as "company.mail") for your Default Domain Name. When configuring your server in this way it may be necessary to use the Header Translation 70 feature, and/or the Domain Name Replacement Engine 87, to enable proper mail distribution.

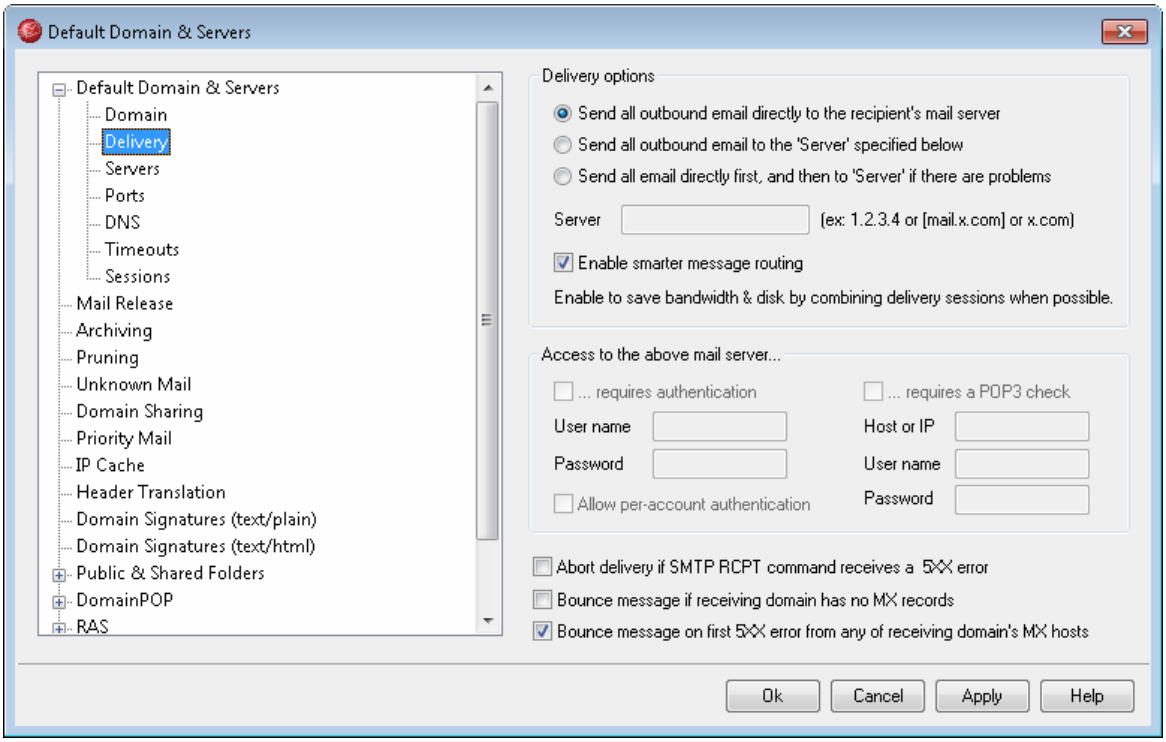
**FQDN for this host**
This value is the Fully Qualified Domain Name (FQDN) that will be used in the SMTP HELO/EHLO instruction when sending mail. In most cases, this will be your Default Domain name. An IP literal syntax is allowed in this option (for example, "[192.0.2.0]").

**Domain IP**
This is the Default Domain's IP address.

**Restrict connections to this IP**
Enabling this option causes MDaemon to restrict the Default Domain's connections to the specific IP address found in the *Domain IP* text box. Ordinarily, this control will only need to be used in certain circumstances when hosting multiple domains. By default this only restricts inbound connections to the specified IP address. If you wish to restrict outbound connections as well, activate the *Enable outbound IP binding for domains using inbound IP binding* option located under: "Preferences » System 195."

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.1.2 Delivery




#### Delivery Options

**Send all outbound email directly to the recipient's mail server**
When this option is chosen, MDaemon will attempt to deliver all mail directly instead of passing it to another host. MDaemon will place undeliverable messages into its retry system and continue to attempt to deliver them according to the parameters and time intervals that you set on the Retry Queue 482 screen of the Mail Queues dialog. To access this screen from MDaemon's menu bar, click "Queues » Mail Queues... » Retry Queue".

**Send all outbound email to the 'Server' specified below**
Select this option if you want all outbound email, regardless of its destination domain, to be spooled to another host or server for routed delivery. If selected, all outbound email will be sent to the domain or host specified in the *Server* option below. Typically, this feature is useful during high volume periods when direct message delivery would result in an excessive taxation of server resources. If a message cannot be delivered to the designated server then it will be moved into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 482 screen of the Mail Queues dialog.

**Send all email directly first, and then to 'Server' if there are problems**
Click this option if you want to spool only undeliverable outbound email to the domain or host specified in the *Server* option below. Undeliverable mail is email destined for hosts that could not be resolved to an actual IP address (such as an unregistered gateway to a remote network) or email destined for a host that was

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

resolved properly but could not be connected to directly or is refusing direct connections. Rather than return such mail to its originator, this option causes MDaemon to pass the message off to a more powerful MTA. Sometimes the mail system run by your ISP may have routed methods of mail delivery to which your local server may not have direct access. If a message cannot be delivered to the designated server then it will be moved to into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 482 screen of the Mail Queues dialog. At each subsequent delivery attempt, MDaemon will again first try to deliver the message directly to its recipient and then to the designated domain or host.

**Server**
Specify your ISP or mail host's name or IP address here. This is generally the SMTP server on your ISP.

Do not enter MDaemon's Default Domain or IP addresses into this text box. This entry should be an ISP or other mail server that can relay mail for you.

**Enable smarter message routing**
By default, whenever possible MDaemon will maintain a single copy of each message destined for multiple recipients and use multiple RCPT commands to deliver the message. This saves on disk space and bandwidth. For example, if enabled, this option will always operate whenever there is a single message addressed to multiple recipients at the same domain. Also, if you are using the "*Send all outbound email to the 'Server' specified below*" delivery option, which sends all your outbound mail to a single designated host, MDaemon will store a single copy of each message and use multiple RCPT commands even when recipients belong to different domains.

## Access to the above mail server...

As an added security measure, some smart hosts or ISPs require you to authenticate using login credentials or perform a POP mail check before you are allowed to send mail through their servers. If your ISP or mail host requires this then use these options to specify your login or POP credentials.

**...requires authentication**
Click this check box if the ISP or host to which you will be sending messages requires authentication. Enter your login credentials below. These login credentials will be used for all outbound SMTP messages sent to the server specified above. If, however, you choose to use the *Allow per-account authentication* option below, then MDaemon will authenticate to your host separately for each message, using the sending account's *Optional smart host user/password* setting designated on the Account Details 343 screen of the Account Editor.

**User name**
Enter your user name or login here.

**Password**
Use this option to specify your ISP or mail host login password.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...requires a POP3 check**
If your ISP or mail host requires a POP3 check before it will accept messages from you, then click this check box and enter your required credentials below.

**Host or IP**
Enter the host or IP address to which you wish to connect.

**User name**
This is the POP account's login or account name.

**Password**
This is the POP account's password.

**Allow per-account authentication**
Click this checkbox if you wish to use per-account authentication for outbound SMTP messages sent to the *Server* specified above. Instead of using the *User name* and *Password* credentials provided here, each account's *Optional smart host login/password* settings designated on the Account Details 343 screen of the Account Editor will be used for authentication. If, however, no *Optional smart host login/password* settings have been designated for a given account, then the above credentials will be used for that account.

If you wish to configure *per-account authentication* to use each account's *Email password* instead of its optional *Smart host password*, then you can do so by editing the following key in the `MDaemon.ini` file:

```
[AUTH]
ISPAUTHUsePasswords=Yes (default No)
```

Enabling the `ISPAUTHUsePasswords=Yes` option will over time effectively communicate all your accounts' local mail passwords to your smart host. This could pose a risk to mail security, since it is providing sensitive information to another server. You should not use this option unless you are using a smart host that you absolutely trust and you believe it is necessary to do so. Further, you should note that if you use this option and give your users permission to change their *Email password* via WebAdmin or some other means, then changing the *Email password* will also effectively change the *Smart host password*. This could cause smart host authentication to fail for an account when its *Email password* is changed locally but the corresponding *Smart host password* isn't changed at your smart host.

**Abort delivery if SMTP RCPT command receives a 5xx error**
Enable this option if you wish MDaemon to abort its attempt to deliver a message when it receives a 5xx fatal error in response to the SMTP RCPT command. This option is disabled by default.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

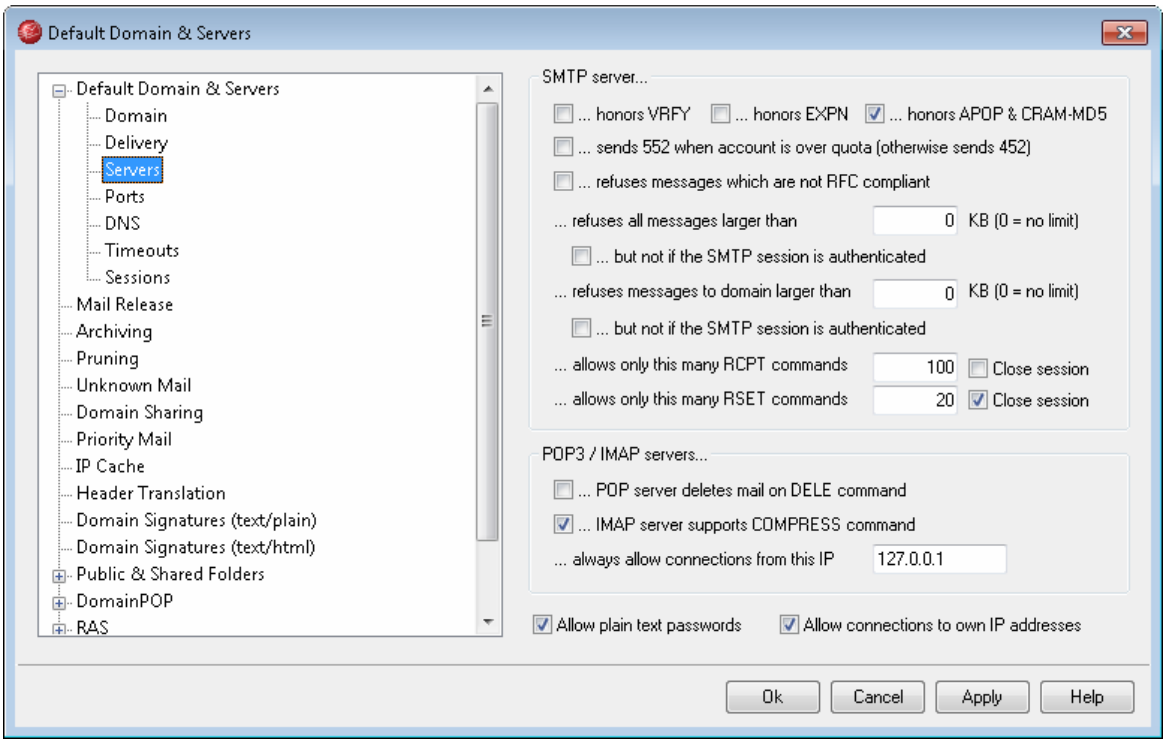
**Bounce message if receiving domain has no MX records**
Ordinarily when MDaemon checks the receiving domain's DNS records, it will look for MX records and then for an A record when no MX records are found. If neither are found then it will bounce the message back to the sender as undeliverable. Click this option if you want MDaemon to immediately bounce the message when no MX record is found, instead of allowing it to then look for an A record also. This option is Disabled by default.

**Bounce message on first 5XX error from any of receiving domain's MX hosts**
When this checkbox is enabled, MDaemon will return/bounce the message when it receives a 5xx fatal error response from an MX host. Consequently, it won't continue trying to deliver the message to any subsequent MX hosts that may be designated for the recipient's domain. If this option is disabled, MDaemon won't bounce the message as long as at least one of the MX hosts returns a 4xx non-fatal error response. This option is enabled by default.

**See:**

**Retry Queue** 482

### 4.1.1.3 Servers




**SMTP Server...**

**...honors VRFY**
Click this switch if you wish to respond to SMTP VRFY commands. This command is

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

sometimes used by servers that use an SMTP call forward or call back feature to attempt to confirm the validity of email addresses on your server. This is disabled by default.

**...honors EXPN**
Click this checkbox if you want MDaemon to honor EXPN commands.

**...honors APOP & CRAM-MD5**
By default MDaemon's servers (POP, IMAP, and so on) honor the APOP and CRAM-MD5 methods of authentication. These methods provide extra security by making it possible for users to be authenticated without sending clear text passwords. Clear this checkbox if you do not wish to allow APOP or CRAM-MD5.

**...sends 552 when account is over quota (otherwise sends 452)**
Enabling this option will cause a 552 response ("Requested mail action aborted: exceeded storage allocation") when delivery is attempted to a recipient whose account exceeds its quota[366]. Normally there would be a 452 response ("Requested action not taken: insufficient system storage").

**...refuse messages which are not RFC compliant**
Enable this option if you wish to reject messages during the SMTP process that are not compliant to RFC internet standards. To pass the compliance test the message must:

1. Be greater than 32 bytes in size (the minimum size necessary to include all required parts).
2. Have a DATE: header.
3. Have either a FROM: or a SENDER: header.
4. Have no more than one FROM: header.
5. Have no more than one SUBJECT: header, though no subject header is required.

Messages using authenticated sessions or from trusted domains or IP addresses are exempt from this requirement.

**...refuses all messages larger than [xx] KB (0=no limit)**
Setting a value here will prevent MDaemon from accepting or processing mail that exceeds a certain fixed size. When this option is enabled MDaemon will attempt to use the ESMTP SIZE command specified in RFC-1870. If the sending agent supports this SMTP extension then MDaemon will determine the message size prior to its actual delivery and will refuse the message immediately. If the sending agent does not support this SMTP extension then MDaemon will have to begin acceptance of the message, track its size periodically during transfer, and finally refuse to deliver the message once the transaction has completed. Use "0" in this option if you do not wish to set a size limit. If you wish to exempt authenticated sessions from SIZE checks, use the "*...but not if SMTP session is authenticated*" option below.

**...but not if the SMTP session is authenticated**
Check this box if you wish to exempt messages from the message size limitation

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

when the SMTP session is authenticated.

**...refuses messages to domain larger than [xx] KB (0=no limit)**
Use this option if you wish to refuse messages to the Default Domain that are larger than the size designated. Use "0" in this option if you do not wish to limit message size. There is an equivalent option located on the Domain Manager[108] for refusing messages to your other domains. If you wish to exempt authenticated sessions from SIZE checks, use the "*...but not if SMTP session is authenticated*" option below.

**...but not if SMTP session is authenticated**
Use this option if you wish to exempt authenticated sessions from the domain-specific message size limit.

**...allows only this many RCPT commands [xx] (RFC says 100)**
Use this option if you wish to limit the number of RCPT commands that can be sent per message. Use "0" if you do not wish to set a limit.

**Close session**
Check this box if you wish to close the session immediately if the maximum allowed number of RCPT commands is reached.

**...allows only this many RSET commands [xx]**
Use this option if you wish to set a maximum number of RSET commands allowed in an SMTP session (default is 20). Use "0" if you do not wish to set a limit.

**Close session**
Check this box if you wish to close the session immediately if the maximum allowed number of RSET commands is reached.

## POP3 / IMAP Servers

**...POP server deletes mail on DELE command**
Click this option if you wish MDaemon to delete messages immediately when they are retrieved and the DELE command is received, even if the POP session does not complete properly.

**...IMAP server supports COMPRESS command**
Click this box if you wish to support the IMAP COMPRESS extension (RFC 4978), which compresses all data sent to and from the client. COMPRESS will increase CPU and memory usage per IMAP session.

**...always allow connections from this IP**
The POP and IMAP servers will always accept connections from the IP Address entered into this field regardless of screening and shielding settings.

---

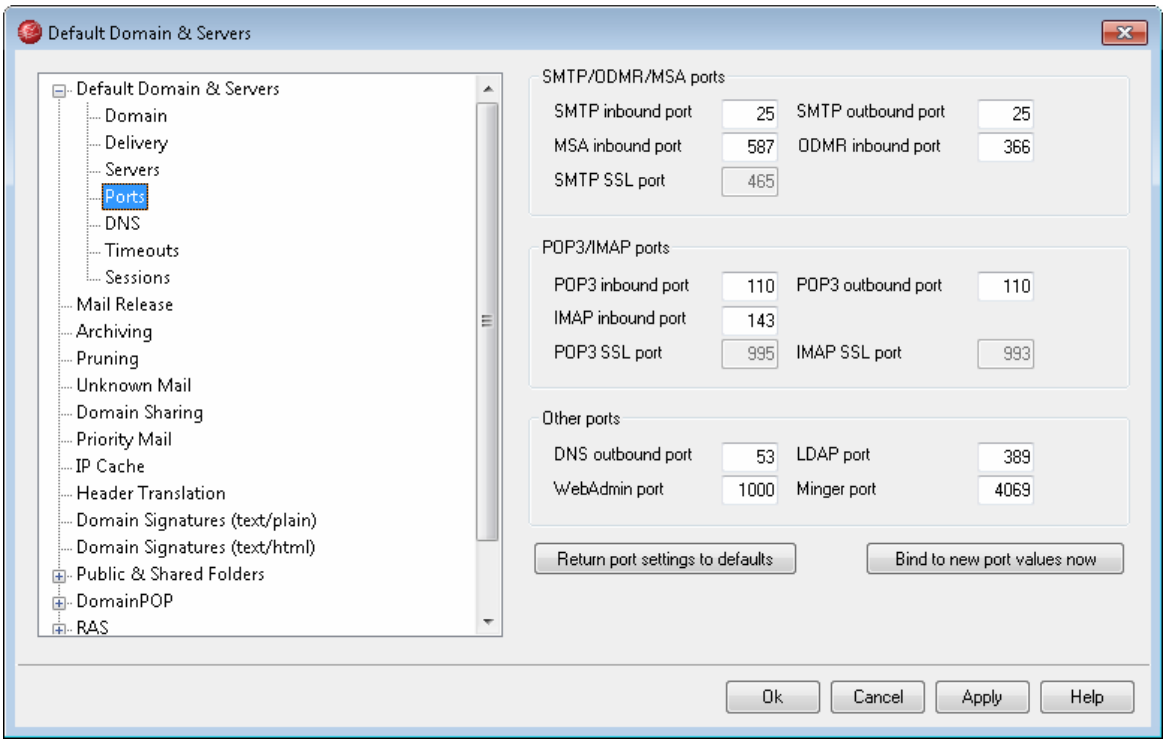
**Allow plain text passwords**
This option governs whether or not MDaemon will accept passwords sent in plain text to the SMTP, IMAP, or POP3 servers. If disabled, the `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN`, and `SMTP AUTH LOGIN` commands will

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

return an error unless the connection is using SSL.

**Allow connections to own IP addresses**
When this option is enabled, MDaemon can connect to itself.

### 4.1.1.4 Ports




**SMTP / ODMR / MSA Ports (some features require MDaemon PRO)**

**SMTP inbound port**
MDaemon will monitor this TCP port for incoming connections from SMTP clients. This is the main SMTP port, which in most cases should be left at the default setting of port 25.

**SMTP outbound port**
This port will be used when mail is sent to other SMTP servers.

**MSA inbound port**
This is a Message Submission Agent (MSA) port that can be used by your users as an alternative to the *SMTP inbound port* specified above. Transmission on this port requires AUTH, therefore users sending on that port must configure their mail clients appropriately to ensure that their connections are authenticated. Further, because some ISPs block port 25, your remote users might be able to circumvent that restriction by using the MSA port instead. If you do not wish to designate an MSA port then set the value to "0" to disable it.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Connections to the MSA port are exempt from PTR and reverse lookups, Host and IP screening, the IP Shield, and Tarpitting. MSA port connections continue to utilize dictionary attack connection limiting.

**ODMR inbound port**
MDaemon will monitor this port for incoming On-Demand Mail Relay (ODMR) connections, such as `ATRN` from Gateway Domains.

**SMTP SSL port**
This is the port dedicated to SMTP mail sessions using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 309 for more information.

### POP3 / IMAP Ports (some features require MDaemon PRO)

**POP3 inbound port**
MDaemon will monitor this port for incoming connections from remote POP clients.

**POP3 outbound port**
This port will be used when MDaemon retrieves mail from POP3 servers.

**IMAP inbound port**
MDaemon will monitor this port for incoming IMAP requests.

**POP3 SSL port**
This is the port dedicated to POP3 mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 309 for more information.

**IMAP SSL port**
This is the port dedicated to IMAP mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 309 for more information.

### Other Ports

**DNS outbound port**
Enter the Port you want MDaemon to use for sending and receiving datagrams to the DNS server.

**LDAP port**
MDaemon will post database and address book information to your LDAP server on this port.

See: LDAP Address Book Support 96

**WebAdmin port**
This is the port that MDaemon will monitor for WebAdmin 132 connections.

**Minger port**
This is the port that the Minger 422 server will monitor for connections.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

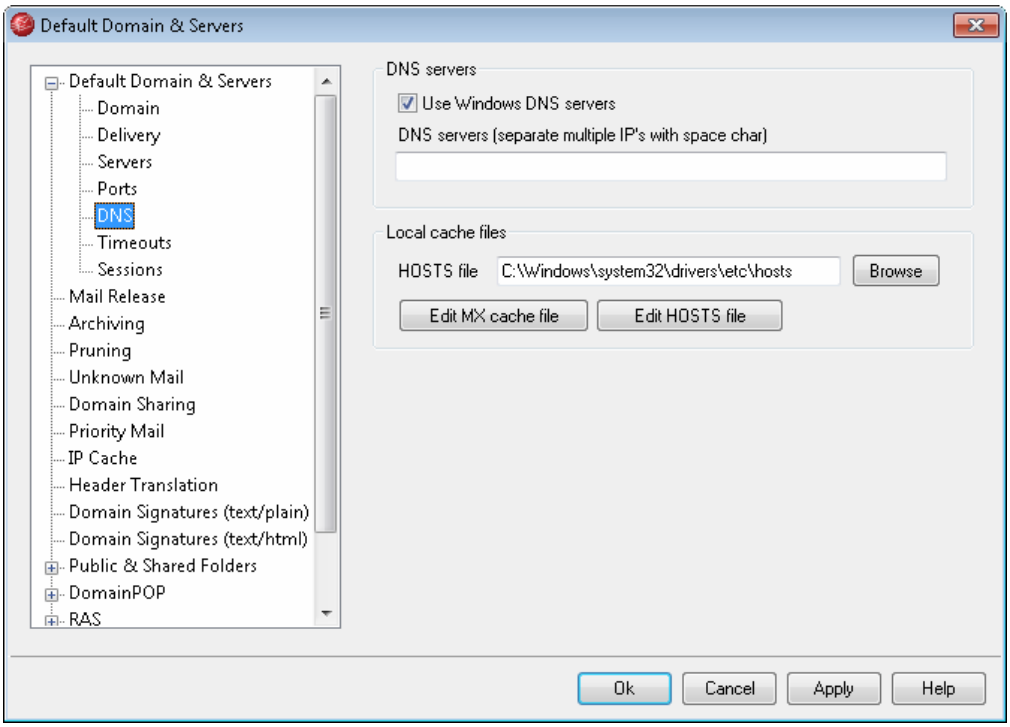
**Return port settings to defaults**
This button returns all the port settings to their standard values.

**Bind to new port values now**
When you alter the values of any of the port settings you will need to press this button to have your changes take immediate effect. Otherwise, your changes will not be put into place until the next time the server is started.

The preceding port settings are critical for proper server operation and should not be altered unless you are certain that you must do so. Being able to configure the ports that MDaemon uses will allow you to configure the server to operate with proxy systems or other software services that require certain port numbers.

An IP address (a machine) has only one of each available port. If one program attempts to gain access to a port that is already in use by another program, an error message will inform the user that the requested address (IP:PORT) is already in use.

### 4.1.1.5 DNS




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### DNS Servers

**Use Windows DNS servers**
When this option is selected, MDaemon will use all DNS servers found within your Windows TCP/IP configuration. MDaemon will try each DNS server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you include additional DNS servers in the *DNS Servers* option below, MDaemon will try those servers as well. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

**DNS servers (separate multiple IPs with space char)**
MDaemon will use all DNS servers specified here when performing DNS lookups (separate multiple IP addresses with a space). MDaemon will try each server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you enable the *Use Windows DNS servers* option above, MDaemon will also query all DNS servers found within your Windows TCP/IP configuration. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

### Local Cache Files

**Hosts file...**
Before querying the DNS servers, MDaemon will first attempt to resolve an address by processing the Windows HOSTS file. If this file contains the IP address of the domain in question, MDaemon will not need to query the DNS server.

You must enter the complete path and filename rather than just the filename. MDaemon will attempt to use the following value as the default location of this file:

[drive]:\windows\system32\drivers\etc\hosts

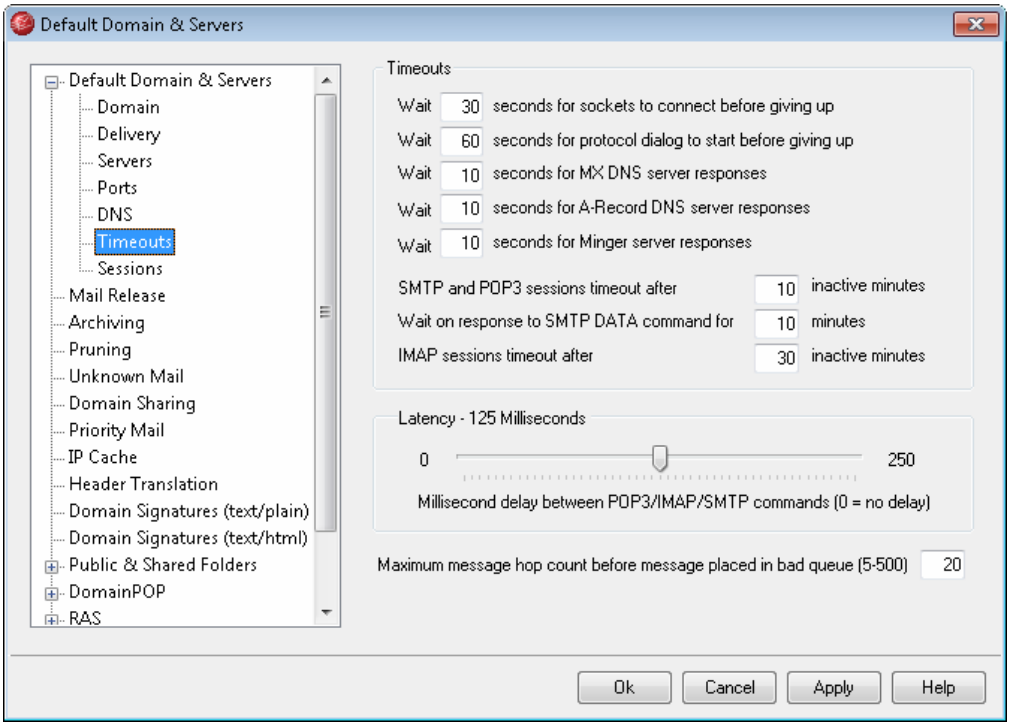
The HOSTS file is a Windows file that contains the A-record or primary IP address for domain names. MDaemon also allows you to specify MX-record IP addresses within a file called MXCACHE.DAT. This file can be found within the MDaemon\APP\ subdirectory. Load the MXCACHE.DAT file into a text editor and read the comments at the top of the file for more information.

**Edit MX cache file**
Click this button to view or edit the MXCACHE.DAT file with a text editor.

**Edit hosts file**
Click this button to view or edit the HOSTS file with a text editor.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.1.6 Timeouts




## Timeouts

**Wait xx seconds for sockets to connect before giving up**
After initiating a connection request MDaemon will wait this many seconds for the remote system to accept the connection. If the remote system does not respond within this time frame, MDaemon will send the message to a specified *Server* or place it into the retry system, depending upon which option you have chosen on the Domain 41 screen of the Default Domain editor.

**Wait xx seconds for protocol dialog to start before giving up**
Once a connection has been established with a remote host, this is the number of seconds that MDaemon will wait for the remote host to begin the SMTP or POP3 protocol dialog. If the remote host does not begin the protocol session within this time frame, MDaemon will send the message to a specified *Server* or place it into the retry system, depending upon which option you have chosen on the Domain 41 screen of the Default Domain editor.

**Wait XX seconds for MX DNS server responses**
While using DNS services to resolve 'MX' hosts for remote domains, MDaemon will wait for responses to its 'MX' queries for this number of seconds. If the DNS server does not respond within this time frame MDaemon will attempt to deliver the message to the IP address specified in the remote host's 'A' DNS record. If that attempt fails, MDaemon will send the message to a specified *Server* or place it into the retry system, depending upon which option you have chosen on the Domain 41 screen of the Default Domain editor.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Wait XX seconds for A-Record DNS server responses**
This timer governs how long MDaemon will wait while attempting to resolve a remote host's IP address. If the attempt fails, MDaemon will send the message to a specified *Server* or place it into the retry system, depending upon which option you have chosen on the Domain 41 screen of the Default Domain editor.

**Wait XX seconds for Minger server responses**
This the the number of seconds that MDaemon will wait for a response from a Minger 422 server.

**SMTP and POP3 sessions timeout after XX inactive minutes**
If a successfully connected and operating session remains inactive (no i/o) for this length of time, MDaemon will abort the transaction. MDaemon will try again at the next scheduled processing interval.

**Wait on response to SMTP DATA command for XX minutes**
This option governs how long MDaemon will wait for the "`250 Ok`" response after sending the `DATA` command during the SMTP process. Since some receiving servers perform lengthy anti-spam, anti-virus, or other necessary operations at that time, this option can be used to give them time to complete those tasks. The default is 10 minutes.

**IMAP sessions timeout after xx inactive minutes**
If an IMAP session has no activity for this number of minutes, MDaemon will close the session.

## Latency

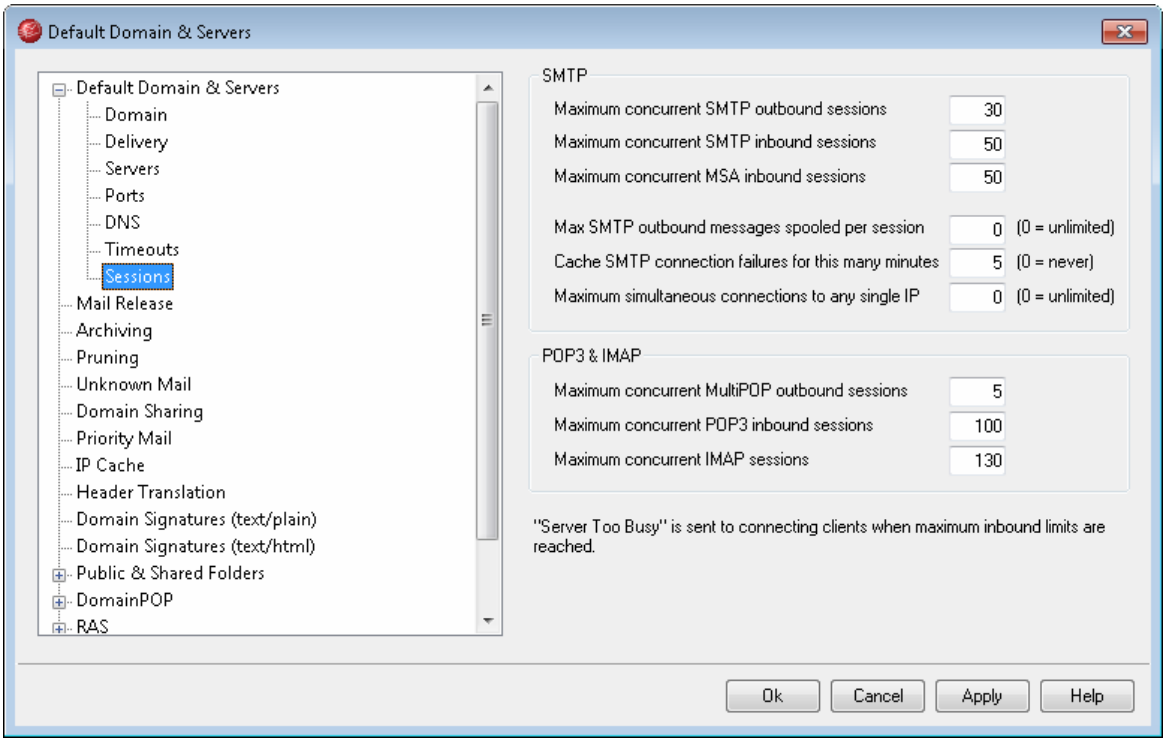
**Latency – xx milliseconds**
This is the delay in milliseconds between POP/SMTP/IMAP protocol commands. This is useful for preventing high-speed connections from processing data faster than the recipient can extract it. This delay takes effect only during the POP/SMTP/IMAP protocol command sequence – the actual transfer of a mail message file is already fully buffered.

## Loop Detection and Control

**Maximum message hop count before message placed in bad queue (5-500)**
RFC standards stipulate that a mail server must stamp each message each time that it is processed. These stamps can be counted and used as a stopgap measure against recursive mail loops that can sometimes be caused by errant configurations. If undetected, these looping message delivery cycles will consume your resources. By counting the number of times the message has been processed, such messages can be detected and placed in the bad message directory. The assumption is that if a message hasn't reached its recipient after being processed by a given number of mail servers then there is probably a mail loop in progress. Most likely, the default setting of this control should be sufficient to prevent mail loops and will not need to be changed.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.1.7 Sessions




#### SMTP

**Maximum concurrent SMTP outbound sessions**
The value entered here represents the maximum possible outbound SMTP sessions that will be created when it is time to send outbound mail. Each session will send outbound messages until either the queue is empty or the *Maximum SMTP outbound messages spooled per session* setting has been reached. For example, if the outbound mail queue has twenty messages waiting when it is time to send mail and the value of this setting is five, then five sessions will be simultaneously created and each will consecutively deliver four messages.

This option is set to 30 by default, but you may wish to experiment with the number of sessions in order to find the setting that will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded or your Windows machine will run out of resources and you will lose delivery efficiency. Remember, each SMTP session created by MDaemon will deliver messages consecutively and therefore four sessions delivering two messages each might perform better and faster than eight threads delivering only one message each. A good place to start would be five to ten threads when using a 56k modem and twenty to thirty for broadband

**Maximum concurrent SMTP inbound sessions**
This value controls the number of concurrent inbound SMTP sessions that the server will accept before it begins responding with a "Server Too Busy" message. The default value is 50.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Maximum concurrent MSA inbound sessions**
Use this option to designate the maximum number of concurrent mail submission agent (MSA) inbound sessions allowed.

**Maximum SMTP outbound messages spooled per session**
This setting places a limit on the number of individual messages that each session will send before it stops delivering mail and frees itself from memory. Ordinarily, you should leave this control set to zero, which will cause each session to continue delivering messages until the queue is empty.

**Cache SMTP connection failures for this many minutes (0 = never)**
When an SMTP connection to a given host fails, MDaemon will cease trying to connect to that host for the number of minutes specified in this option. This can prevent MDaemon from needlessly attempting to connect to a problem host over and over again when, for example, it has multiple messages designated for that host and yet discovers that it is down when making the first delivery attempt. The default setting is "5" minutes. Use "0" if you do not wish to cache SMTP failures.

**Maximum simultaneous connections to any single IP (0 = unlimited)**
Use this option to limit the number of simultaneous connections that will be allowed to a single IP address during mail delivery. Use "0" if you do not wish to limit simultaneous connections.

This option is useful to prevent making too many connections at once to various IP addresses. During delivery, if a message would require a connection to an IP that would exceed this connection limit, then the connection is skipped and the next MX host (or smart host) is used. If no additional hosts are available the message is queued for the next delivery cycle. By default, this option is disabled, which preserves existing behavior. Also by default, connections to trusted IP addresses are exempt from this feature. However, if you'd like to enforce it for trusted IPs you can set the following in the `MDaemon.ini` file:

```
[Sessions]
TrustedIPsUseConnectionLimit=Yes (default No)
```

Also by default, connections to IP addresses reserved for intranet use are exempt from this feature. These are `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, and `172.16.0.0/12`. However, if you'd like to enforce it for reserved IP addresses you can set the following in the `MDaemon.ini` file:

```
[Sessions]
ReservedIPsUseConnectionLimit=Yes (default No)
```

### POP3 & IMAP

**Maximum concurrent MultiPOP outbound sessions**
The value entered here represents the maximum possible outbound POP sessions that will be created when it is time to collect MultiPOP mail. Each session will collect this type of mail until all MultiPOP servers have been processed, and all mail has been collected. For example, if there are fifteen MultiPOP sessions amongst all of your users and the value of this setting is set to three, then each session will collect mail from five MultiPOP sources.

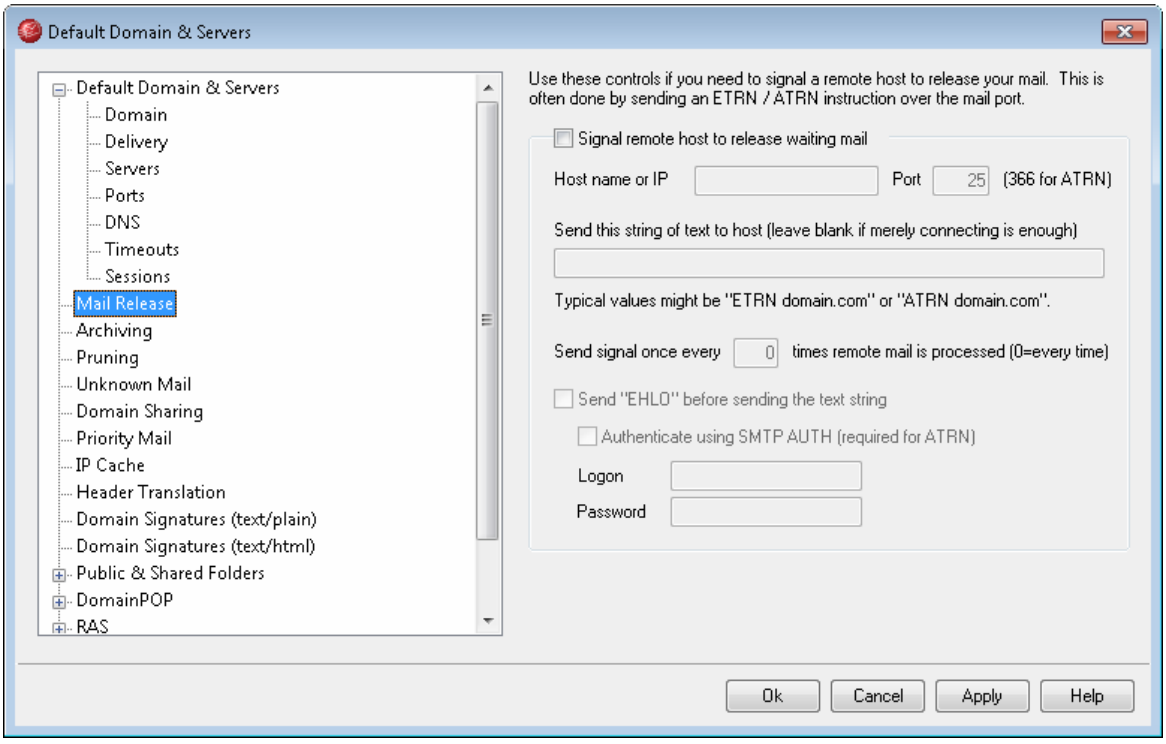
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

You should experiment with the number of sessions to determine what number will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded, or your Windows machine will run out of resources and you will lose processing efficiency. Remember that each POP sessions created by MDaemon will collect mail until all sources have been exhausted. Therefore, four sessions collecting mail from twenty sources might perform better and faster than twenty sessions collecting from a single source.

**Maximum concurrent POP3 inbound sessions**
This value controls the maximum number of concurrent POP inbound mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

**Maximum concurrent IMAP sessions**
This value controls the maximum number of concurrent IMAP mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

### 4.1.2 Mail Release




**Signal remote host to release waiting mail**
When it is time to process remote mail MDaemon can connect to any server on any port and send any string that you wish to send. This is useful when you need to signal a remote server to release your mail by sending some string to them. For example, `ATRN`, `ETRN`, or `QSND`. You can also use this feature when a `FINGER` or `TELNET` session is briefly required in order for your remote host or ISP to determine

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

that you are online.

**Host name or IP**
This is the host that will be signaled to release your mail.

**Port**
Enter the port on which you wish to make the connection. The default is 25 (the SMTP port), which is appropriate for the ETRN or QSND signaling method. Port 366 is typically used for ATRN, and port 79 is used for FINGER.

**Send this string of text to host (leave blank if merely connecting is enough)**
This control is for specifying the text string that needs to be sent in order for your mail to be released. For example, the ETRN method requires the text "ETRN" followed by the domain name of the site being queued. Other methods require different text to be sent. Consult your ISP if you need more information on what to send to unlock your mail queue. If you have a choice of the method to use, we recommend using On-Demand Mail Relay (ODMR) 59 whenever possible. ODMR requires the ATRN command to be used in this option.

**Send signal once every [xx] times remote mail is processed (0=every time)**
By default the dequeue signal will be sent each time that remote mail is processed. Entering a number into this control will prevent the dequeue signal from being sent every time. It will be sent every x number of times as designated. For example, setting this value to "3" would cause the signal to be sent every third time that remote mail is processed.

**Send "EHLO" before sending the text string**
If you enable this checkbox then you should be connecting to an SMTP server to signal release of your mail. This switch causes an SMTP session to be initiated with the specified host and allows the session to progress just beyond the SMTP "EHLO" stage before sending the unlock string.

**Authenticate before sending the text string (required for ATRN)**
As a security measure, some hosts or servers require clients to authenticate using ESMTP AUTH before releasing waiting messages. If this is the case for your mail host, click this checkbox and enter the required authentication credentials below.

Authentication is required when using the ATRN command to dequeue your email.

**Logon**
Enter the AUTH logon parameter here that is required by your host.

**Password**
Enter the AUTH password here.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

#### 4.1.2.1 On-Demand Mail Relay (ODMR)

When you require a queue/dequeue method for hosting and releasing your email, we recommend using On-Demand Mail Relay (ODMR) whenever possible. This method is superior to ETRN and other methods in that in requires authentication before mail is released. Further, it utilizes an ESMTP command called ATRN that does not require the client to have a static IP address, because it immediately reverses the flow of data between the client and server, releasing the messages without having to make a new connection to do so (unlike ETRN).

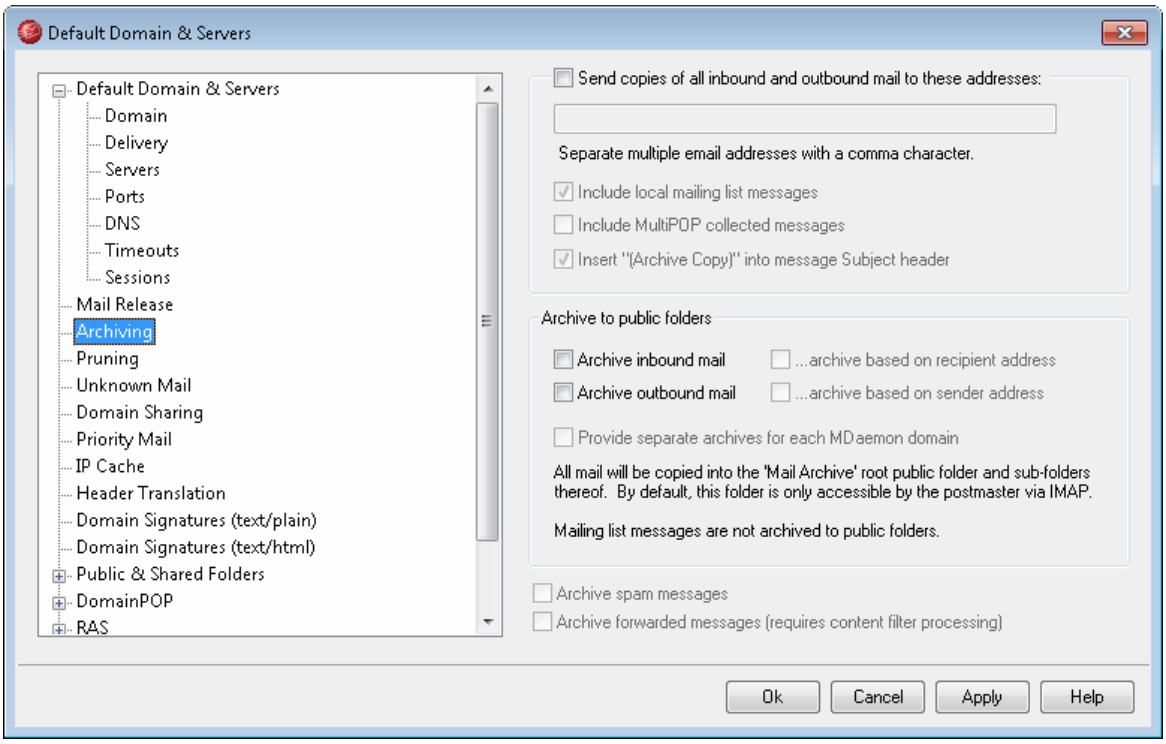
MDaemon fully supports ODMR on the client side via using the ATRN command and authentication controls on the Mail Release 57 screen, and on the server side using the Domain Gateways features on the Dequeuing 466 screen of the Gateway Editor.

Some mail servers do not support ODMR, therefore you should check with your provider before attempting to use it.

**See:**

**Gateway Editor » Dequeuing** 466

### 4.1.3 Archiving




**Send copies of all inbound and outbound mail to these addresses**
Enter one or more addresses to which you wish to send archival messages. Multiple addresses must be separated by a comma. You may specify local and remote addresses and address aliases.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Include local mailing list messages**
When this option is enabled, archived mail will include your mailing list messages.

**Include MultiPOP collected messages**
Enable this option if you wish to archive messages collected through MDaemon's MultiPOP 369 feature.

**Insert "(Archive Copy)" into message Subject header**
When this option is enabled, "(Archive Copy)" will be inserted in the `Subject:` header of archived mail.

### Archive to Public Folders

**Archive inbound mail**
Click this check box to save a copy of all inbound messages into the Mail Archive root public folder and its subfolders. By default, this folder is accessible only by the Postmaster via IMAP. If you want to alter the permissions or grant access to more users you can do so by using the Access Control List 79 reached from the Folder Listing 77 screen of Public & Shared Folders.

**...archive based on recipient address**
Click this option if you want the inbound mail archive to be categorized by the recipient's email address.

**Archive outbound mail**
Click this check box to save a copy of all outbound messages in the Mail Archive public folder. By default, this folder is only accessible only by the Postmaster via IMAP. If you want to alter the permissions or grant access to more users you can do so by using the Access Control List 79 reached from the Folder Listing 77 screen of Public & Shared Folders.

**...archive based on sender address**
Click this option if you want the outbound mail archive to be categorized by the sender's email address.

**Provide separate archives for each MDaemon domain**
Click this option if you want to maintain a separate archive for each domain.

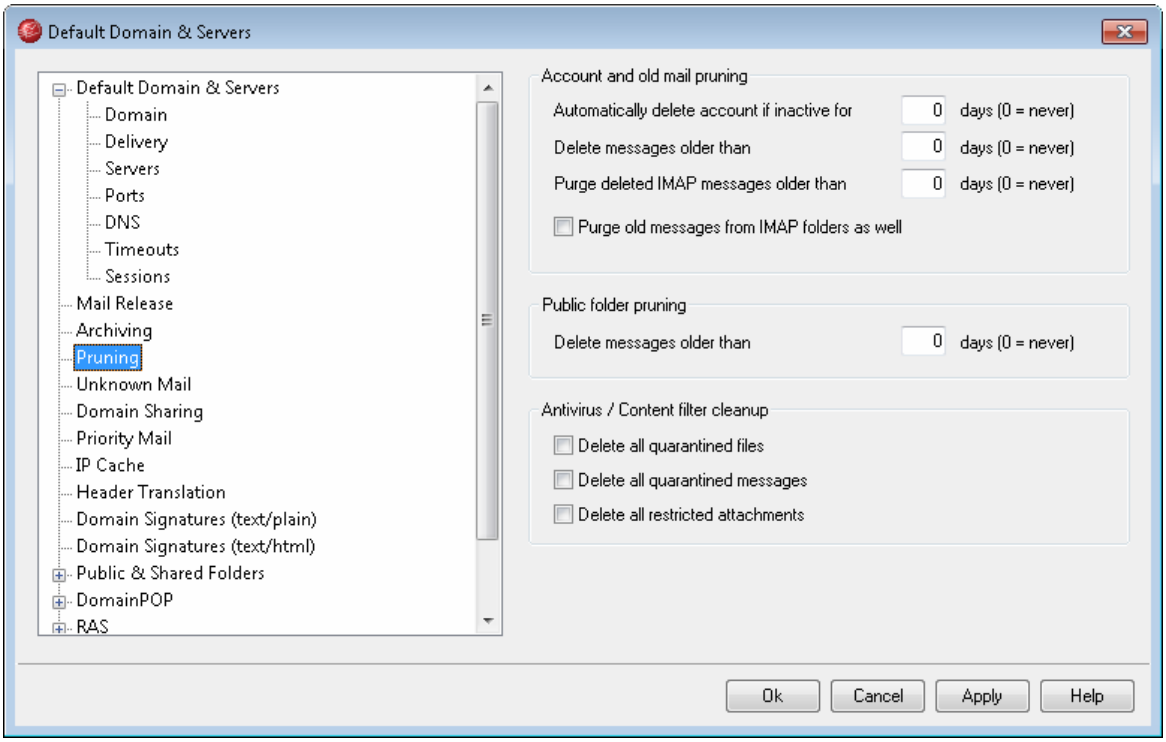
### Archive Settings

**Archives spam messages**
Enable this option if you wish the archives to include messages that are marked as spam.

**Archive forwarded messages (requires content filter processing)**
Enable this option if you want the archives to include messages that are forwarded. By default these are not archived.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.4 Pruning




The options in the first section of this dialog are used to designate when or if inactive accounts or old messages belonging to the default domain will be deleted by MDaemon. Each day at midnight MDaemon will remove all messages and accounts that have exceeded the time limits stated. There are similar controls on the Domain Manager[108] used for setting these limits for your other domains. There are also controls on the Account Editor that can be used to override these settings for individual accounts.

When old messages are pruned, MDaemon will not actually delete them, but will move them to the "...\BADMSGS\[Mailbox]\" folder where they can be manually deleted later by the administrator or a nightly process. **Note:** This only applies to pruned old messages. When an account is pruned, it will be deleted along with its messages instead of moved. See `AccountPrune.txt` in the "...MDaemon\App\" folder for more information and command line options.

#### Account and Old Mail Pruning

The options in this section apply only to the default domain. Use the Domain Manager[108] to configure these settings for other domains.

**Automatically delete account if inactive for XX days (0 = never)**
Specify the number of days that you wish to allow an account belonging to this domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Delete messages older than XX days (0 = never)**
A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

**Purge deleted IMAP messages older than XX days (0 = never)**
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in your users' folders. Messages flagged for deletion longer than this number of days will be purged from their mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

**Delete old messages from IMAP folders as well**
Click this checkbox if you want the "*Delete messages older than...*" control to apply to messages in IMAP folders as well. When this control is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

### Public folder pruning

**Delete messages older than XX days (0=never)**
Specify a number of days in this option if you want old messages to be deleted from Public Folders.

### Antivirus/Content Filter Cleanup

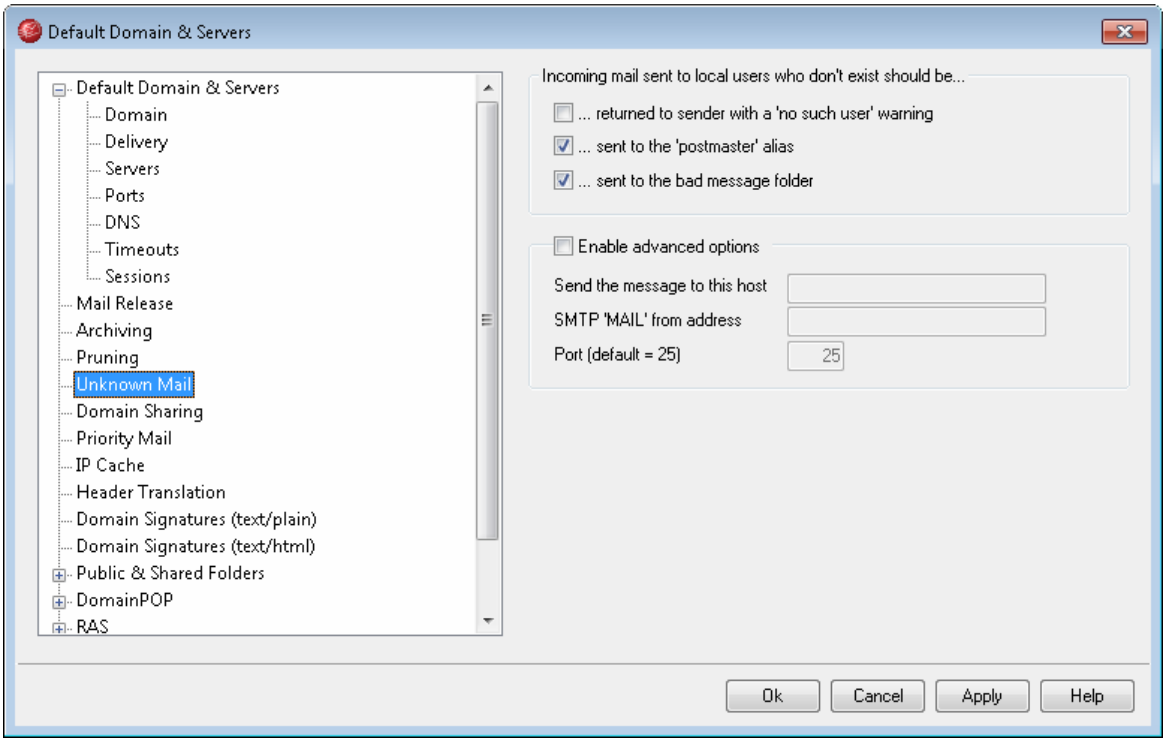
**Delete all quarantined files**
Click this option if you want all quarantined file attachments to be deleted each night.

**Delete all quarantined messages**
Click this option if you want all quarantined messages to be deleted each night.

**Delete all restricted attachments**
Click this option if you want all restricted attachments to be deleted each night.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.5 Unknown Mail




**Incoming mail sent to local users who don't exist should be...**

**...returned to sender with a 'no such user' warning**
When this option is enabled, messages that arrive at the server destined for unknown yet supposedly local users will be returned to the message originator.

**Send message to the "postmaster" user**
By default, messages that arrive at the server destined for unknown yet supposedly local users will be forwarded to whatever user has been aliased as the postmaster. Disable this option if you do not wish to send these messages to the Postmaster.

**Place message in bad message directory**
By default, messages that arrive at the server destined for unknown yet supposedly local users will be routed to the bad message queue. Clear this checkbox if you do not wish to send these messages to the bad message queue.

**Advanced Options**

**Enable advanced options**
Click this checkbox to enable the following advanced mail routing properties.

**Send the message to this host**
If a mail host is specified here, messages addressed to unknown local users will be sent to it.

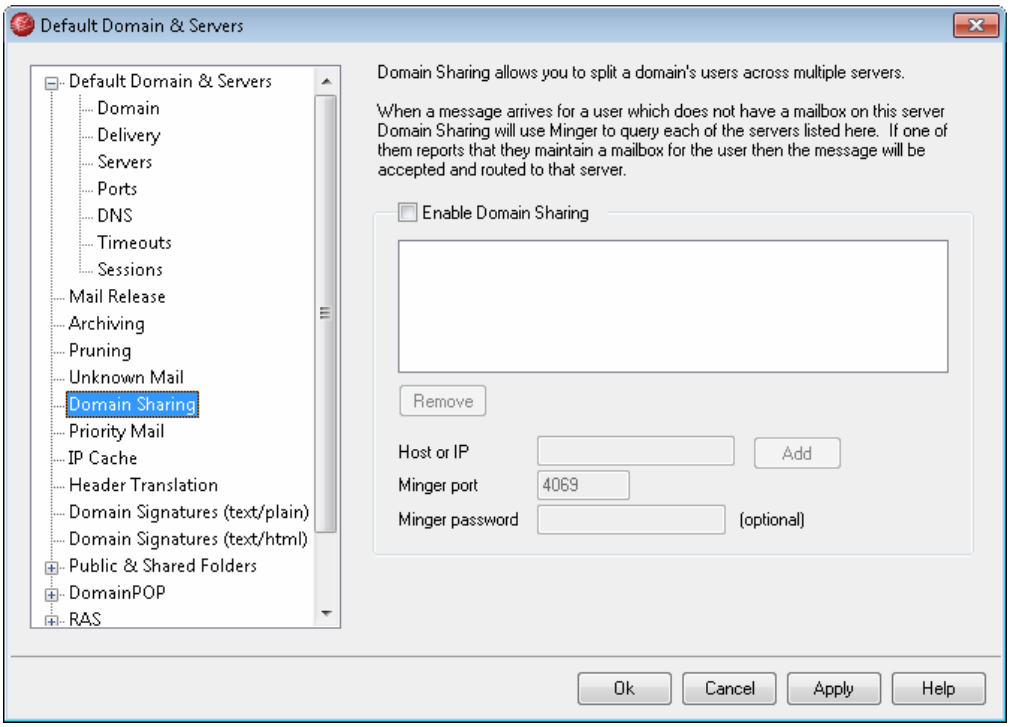
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

The following applies globally anywhere within MDaemon where you are allowed to specify a host to forward, copy, or send email to. If you enclose the host in brackets (e.g. `[example.com]`), MDaemon will skip MX record lookups when delivering to that host. For example, if this option contained "`example.com`" then MX lookups would be performed normally. If, however, that option contained "`[example.com]`" then only the A-record lookup would be performed.

**Use this address in SMTP envelope**
This address will be used in the SMTP "`Mail From:`" statement used during the session handshaking with the accepting host. Normally the sender of the message is used in this portion of the SMTP envelope. If you require an empty command (`MAIL FROM <>`) then enter "`[trash]`" into this control.

**Use this TCP port**
MDaemon will send this message on the TCP port specified here rather than the default SMTP outbound port.

## 4.1.6 Domain Sharing




Domain Sharing is a feature which allows you to split a domain's users across multiple servers. This makes it possible for you to have MDaemon servers running in different locations, all using the same domain names but with different user accounts. One

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

portion of your domains' user accounts are hosted on one server while another portion of them are hosted on one or more other servers. The Domain Sharing dialog is used to specify where each of these other servers is located. Then, when an incoming message arrives for a local user who does not have a local mailbox, Domain Sharing will use Minger to query the other servers in order to discover whether or not that user has an account on one of them. If the address is found to be valid, MDaemon will accept the message and route it to the server where the account is located.

For example, you could have offices in multiple cities and choose to use Domain Sharing to allow every employee to have an email address ending with, "`@example.com`." Each office's MDaemon would host a portion of `example.com's` email, having accounts only for the local employees who work in that office. Then, every office would be configured to use Domain Sharing, so that everyone's messages would get routed to the correct office.

Because Domain Sharing uses Minger 422 to verify addresses, Minger must be enabled and properly configured on each server in order for queries to function. If, however, an error occurs during a Minger query, such as when one of the servers is temporarily unavailable, MDaemon will respond with a "451" temporary error code so that the sending server can try to deliver the message again later. Further, once an address has been verified, it will be cached for five days so that MDaemon can immediately accept future messages for that address and begin attempting to route those messages to the proper host.

Finally, to avoid potential problems that could occur if the same account were created on multiple servers, MDaemon will query all of the Domain Sharing servers before creating any new account.

There is an option called "*Minger verification lookups also trigger Domain Sharing lookups*," located on the Gateway Editor's Options 470 screen. This option can be used to cause MDaemon to also query your Domain Sharing hosts whenever Minger Verification 461 is used by a Gateway.

**Enable Domain Sharing**
Check this box to enable Domain Sharing. After you have enabled Domain Sharing and added all of the Domain Sharing hosts or IP addresses to the list, ensure that you have also enabled and configured Minger 422 so you can respond to queries from those hosts when they attempt to verify your local addresses.

**Remove**
To delete one of your Domain Sharing entries, select it from the list and click this button.

**Host or IP**
Use this box to enter the host or IP address that is sharing one or more of your domains. You can append a colon and port (e.g. `mail.example.com:2525`) if you wish to use a specific, non-default port when sending SMTP messages to the host (this is not the same as the Minger port below).

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Minger port**
This is the port that Minger will use when querying this host. The default port is 4069.

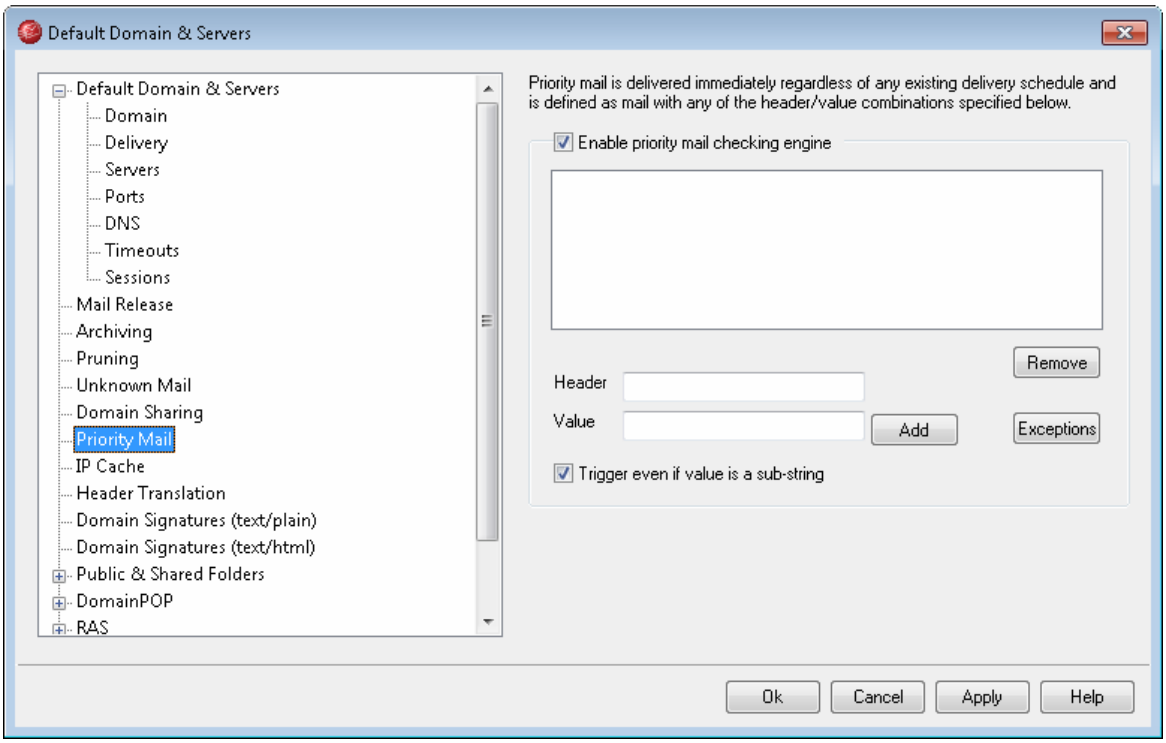
**Minger password (optional)**
If the host that you are adding requires a Minger password, enter it here. Setting up Minger to require a password is optional, but it is recommended.

**Add**
After entering the host or IP, port, and password, click this button to add the new Domain Sharing entry to the list.

**See:**

**Minger** 422
**Default Domain** 41
**Domain Manager** 108

## 4.1.7 Priority Mail




The Priority Mail screen is reached from the "Setup » Default Domain/Servers » Priority Mail" menu selection. It is used to define what constitutes Priority Mail on your system. Priority mail is delivered immediately by MDaemon regardless of scheduled mail processing intervals. When a new message arrives, MDaemon inspects its headers for a set of header/value combinations that you have specified on this dialog. If it finds

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

them, it considers the message a high priority item and attempts to deliver it immediately.

### Priority Mail Engine

**Enable priority mail checking engine**
Check this box to enable the Priority Mail feature. MDaemon will inspect incoming messages for priority status.

**Header**
Enter the message header in this field. Do not include the ending colon character.

**Value**
Enter the value that must be found in the specified header in order for the message to be considered high priority.

**Trigger even if value is a sub-string**
When entering a new Priority Mail setting you may select this feature to enable priority matching of a portion (or sub-string) of a header value. For example, you could create a Priority Mail Setting for the "`To`" header with the value "`Boss`". Then, any email containing "`Boss@anything`" in that header would be considered Priority Mail. If an entry is created without this feature enabled then the value of the header must match the entry exactly; matching only a portion will not be sufficient.

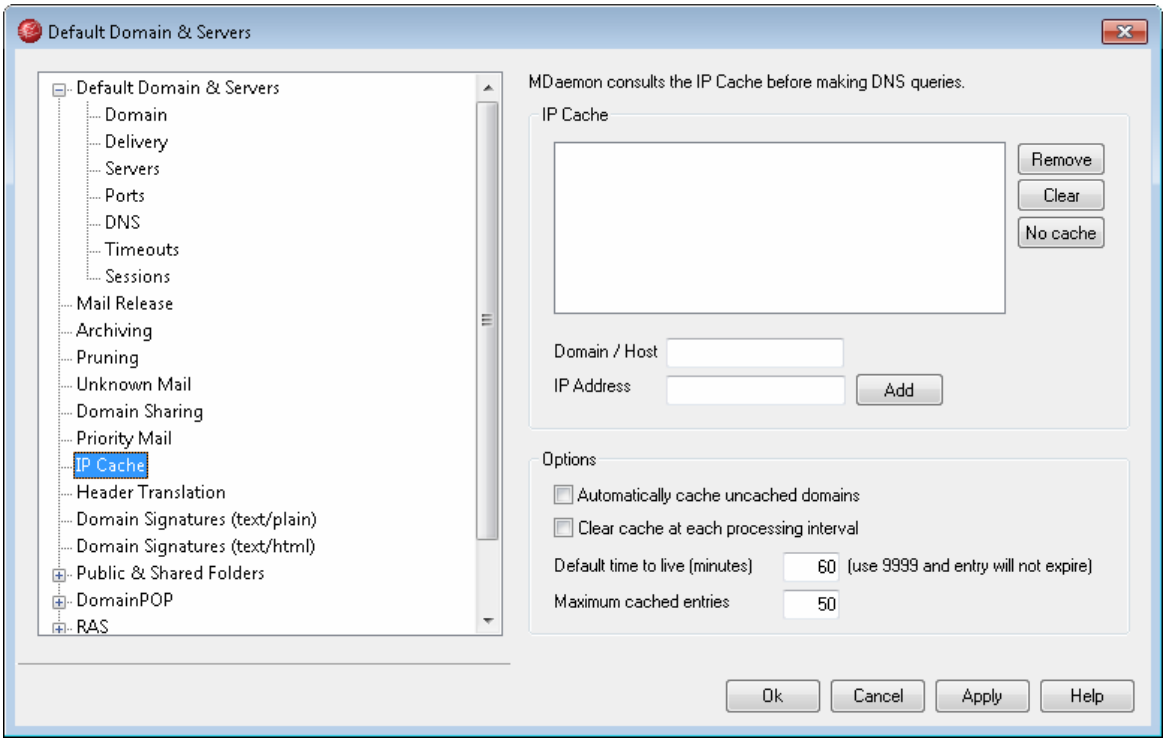
**Add**
After entering the Header/Value information in the specified text boxes, and after specifying whether this entry will apply to sub-strings, click the *Add* button to create the new Priority Mail entry.

**Remove**
Click this button to remove a selected entry from the *Current Priority Mail Settings* window.

**Exceptions**
This allows you to define field/value combinations that will cause a message to be considered an exception to the priority mail settings. This gives you more flexible control over this feature.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.8 IP Cache




In order to speed message delivery and shorten mail processing time, MDaemon caches the IP addresses of all hosts with which it comes in contact. These IPs are stored and then the cache is checked each time MDaemon requires a DNS resolution on a host name. If the host name needing resolution is found in the IP cache then the DNS lookup is skipped, which can save a surprising amount of processing time. The settings in this window allow you to manipulate the parameters under which the cache will operate. You may also manually add and remove entries, set the maximum size of the cache, and designate how long entries will remain cached. The IP Cache can be reached from the "Setup » Default Domain/Servers » IP Cache" menu selection.

#### IP Cache

**Domain / Host**
Enter the domain name or host that you wish to add to the IP cache.

**IP**
Enter the IP address that you wish to add to the IP cache.

**Add**
Once you have manually entered a domain or host and IP address, click this button to add it to the cache.

**Remove**
If you wish to remove a cached IP address from the list, select the entry and then click this button.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Clear**
This button will delete all entries in the cache.

**No cache**
Click this button to bring up a list of domain names and/or IP addresses that you never want MDaemon to add to the IP Cache.

## Options

**Automatically cache uncached domains**
This option governs MDaemon's internal auto-caching engine. If you want MDaemon to cache domains automatically then enable this option. If you want to build the IP Cache yourself, then clear this checkbox.

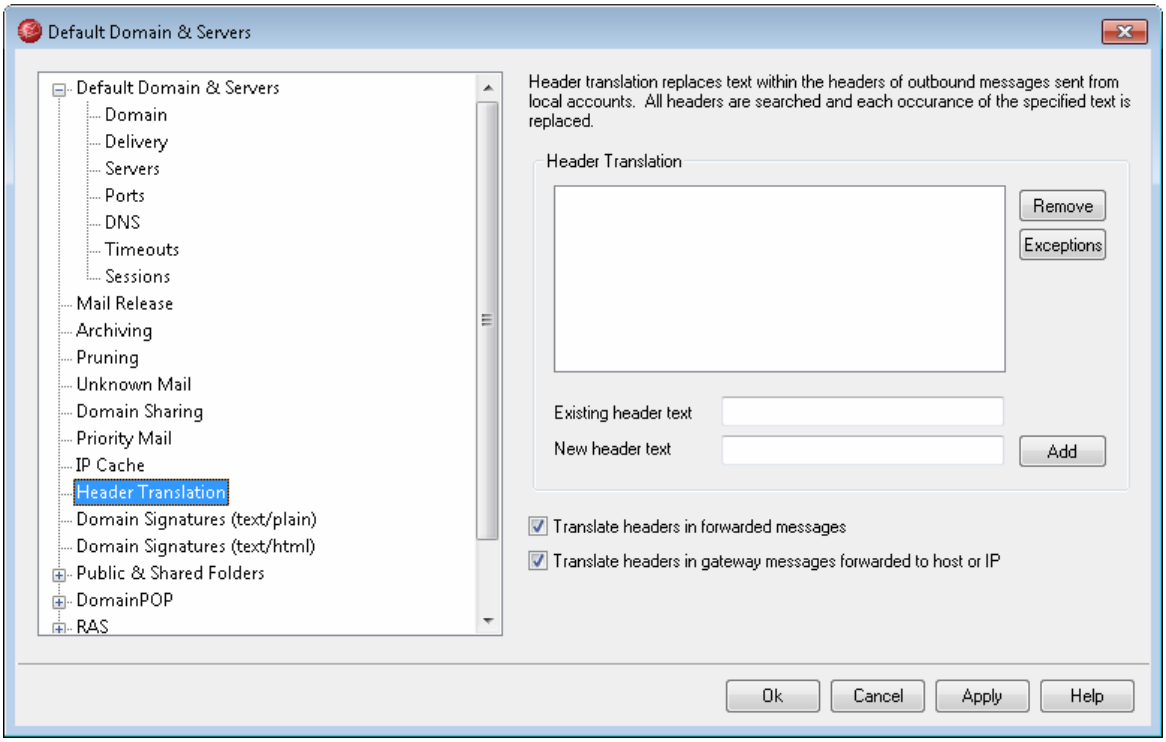
**Clear cache at each processing interval**
If selected, the entire contents of the cache will be flushed at the start of each mail session. This allows the cache to be refreshed at each processing interval.

**Default time to live (minutes)**
This is the default value in minutes that an entry will remain in the IP Cache. Once the entry has been in the IP Cache for this number of minutes, MDaemon will remove it. If you want to set a permanent entry in the IP Cache then designate the *Default time to live* as 9999.

**Max cached entries**
This value determines how large the cache may be. Once this number is reached, the next cache entry will bump the first one out of the cache.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.9 Header Translation




The Header Translation feature can change any portion of text found within a header to a new value whenever a message is detected which must leave your domain destined for a remote host. You specify the text you want to search for and its corresponding replacement value. MDaemon will then search through all the headers in the message and make the replacements. You may also specify headers that MDaemon should **not** modify (such as "Subject:" or "Received:" headers) by clicking the *Exceptions* button on this dialog.

This feature is necessary for some MDaemon configurations in which the local domain name is fictitious or different from the domain name that must appear on outbound mail. In such a situation, Header Translation could be used to change every occurrence of "`@localdomain`" to "`@RemoteDomain`".

#### Header Translations

This list contains the portions of text that MDaemon will scan for in the outbound message headers, and the text that will be substituted when a match is found.

**Remove**
Select an entry in the Current Header Translations list and then click this button to remove it from the list.

**Exceptions**
Click this button to open the Header Translation Exceptions 71 dialog. This dialog is used for specifying any Headers that you wish to be omitted from the Header Translation process.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Existing header text**
Type the text that you want to be replaced when it is found within the headers of any outbound message.

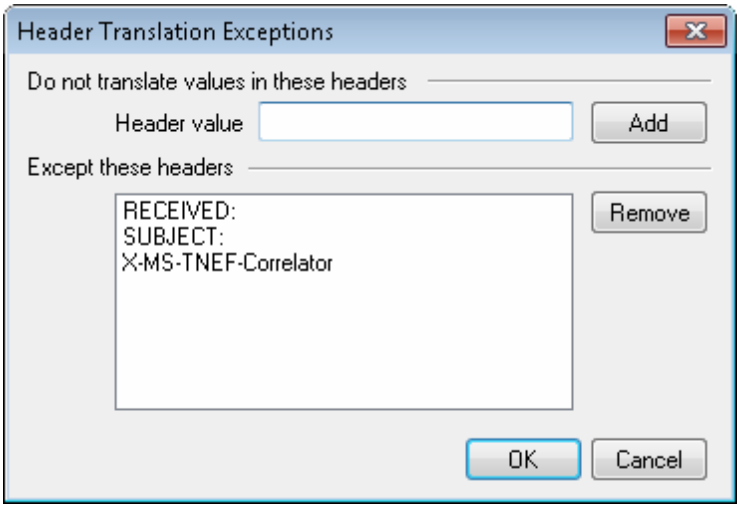
**New header text**
This text will be substituted for that which you specified in the *Existing header text* field.

**Add**
Click this button to add the above text parameters to the *Header Translation* list.

**Translate headers in forwarded messages**
Click this checkbox to cause the header translations to apply also to messages automatically forwarded from a local domain to a non-local domain.

**Translate headers in gateway messages forwarded to host or IP**
Click this check box if you want the headers to be translated in forwarded domain gateway mail. See the Forwarding 465 screen of the Gateway Editor for more information.

### 4.1.9.1 Header Translation Exceptions




**Do not translate values in these headers**

**Header value**
Enter any header that you want to be omitted from the Header Translation 70 process.

**Add**
Click this button to add a new header to the list.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

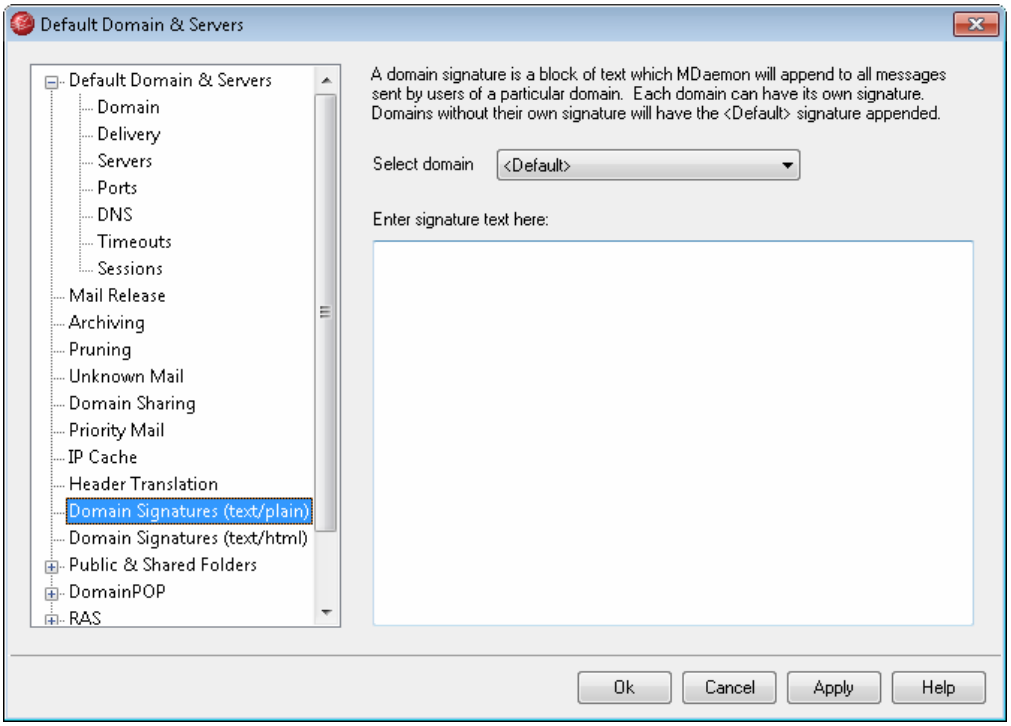
**Except these headers**

MDaemon will not scan these headers when it is substituting header text.

**Remove**

Select a header in the list and then click this button to remove it.

## 4.1.10 Domain Signatures (text/plain)



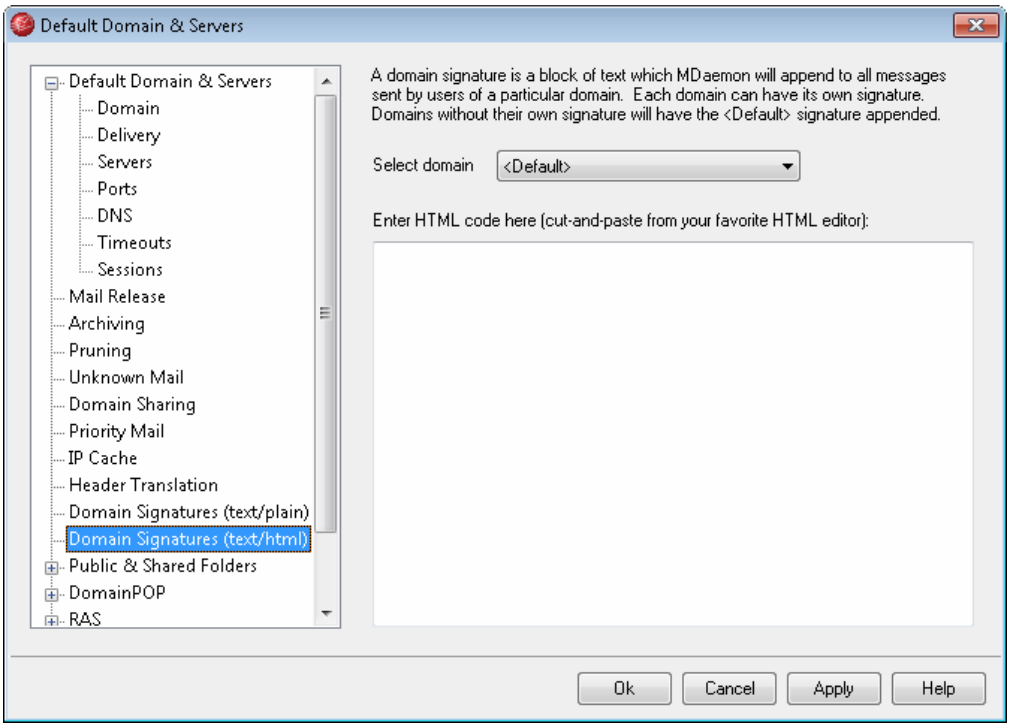

This dialog makes it possible for you to easily create default and per-domain message signature text. If the default signature text is present it will be appended to all messages sent from all local users — unless there is alternate text supplied for the user 's specific domain. When domain-specific text if found, it is given priority over the default text. Domain Signatures are added to the bottom of messages, except for mailing list messages using a footer, in which case the footer will be added below the Domain Signature. You can also use the Account Editor's Signature 375 feature to add individual signatures for each Account. Account signatures will be added just before Domain Signatures.

This option is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the Domain Signatures (text/html) 73 screen to do so. If a signature is included on both screens then MDaemon will use the appropriate one for each part of the multipart message. If no

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

html signature is specified then the text/plain signature will be used in both parts.

### 4.1.11 Domain Signatures (text/html)




Use this screen if you wish to designate an html-encoded signature to append to your users' messages. You can create a default signature and per-domain signatures. If a default signature exists it will be appended to messages sent from local users, except when there is a domain-specific signature supplied for the user's domain. Domain-specific signatures are always given priority over the default signature. Domain Signatures are added to the bottom of messages, except for mailing list messages using a footer, in which case the footer will be added below the Domain Signature. You can also use the Account Editor's Signature 375 feature to add individual signatures for each Account. Account signatures will be added just before Domain Signatures.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor.

This option is for inserting a signature constructed with html code. If you wish to designate a corresponding plain text signature to be used in the text/plain part of multipart messages, use the Domain Signatures (text/plain) 72 screen to do so. If a signature is included on both screens then MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html signature will be converted to plain text for use in the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

text/plain part of the message.

### 4.1.12 Public & Shared Folders

MDaemon supports shared Public and User IMAP folders. Public folders are extra folders that do not belong to any particular account but can be made available to multiple IMAP users. User folders are IMAP folders that belong to individual MDaemon accounts. Each shared folder, whether public or user, must have a list of MDaemon users associated with it, and only members of that access list may access it via WorldClient or an IMAP email client.

When IMAP users access their list of personal folders, shared public folders and shared user folders to which they have been given access will also be displayed. In this way certain mail folders can be shared by multiple users but still require each user's individual logon credentials. Further, having access to a folder doesn't necessarily mean having full read/write or administrative access to it. Specific access rights can be granted to individual users, thus allowing you to set different levels of access for each one. For example, you might allow some users to delete messages while restricting that from others.

Once a public or user IMAP folder has been created you can use the Content Filter to set criteria by which certain messages are moved into that folder. For example, it might be useful to make a filter rule that would cause messages containing `support@example.com` in the `TO:` header to be moved into the `Support` public folder. The Content Filter actions 214 "`Move Message to Public Folders...`" and "`Copy Message to Folder...`" make this possible. For shared user folders, you can use your personal IMAP filters 356 to route specific messages to them. In addition to using Content Filters and IMAP filters, you can associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

For added convenience, the Mailing List editor also contains a Public Folder 447 screen that makes it possible for you to configure a public folder for use with a particular list. If you enable this feature then a copy of each list message will be placed into the specified public folder. All public folders are stored in the `\Public Folders\` directory within the MDaemon directory hierarchy.

#### WorldClient Documents Folders

The WorldClient themes support document sharing using document folders. Document folders have full Access Control List (ACL) 79 support like other shared folders, which can be used to set permissions and sharing rules, and any types of files can be shared through the system. WorldClient users can upload files to their document folders using the built-in tools. When using the LookOut theme, browsers that support the HTML5 Drag and Drop API, such as Chrome and Firefox, can also upload files by dragging them from the desktop into the browser window. Filenames can be searched and renamed, and files can be attached to new messages that are being composed.

You can enable/disable the documents folders (and other shared folders) on a per-domain and per-user basis by editing the `\WorldClient\Domains.ini` file and

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

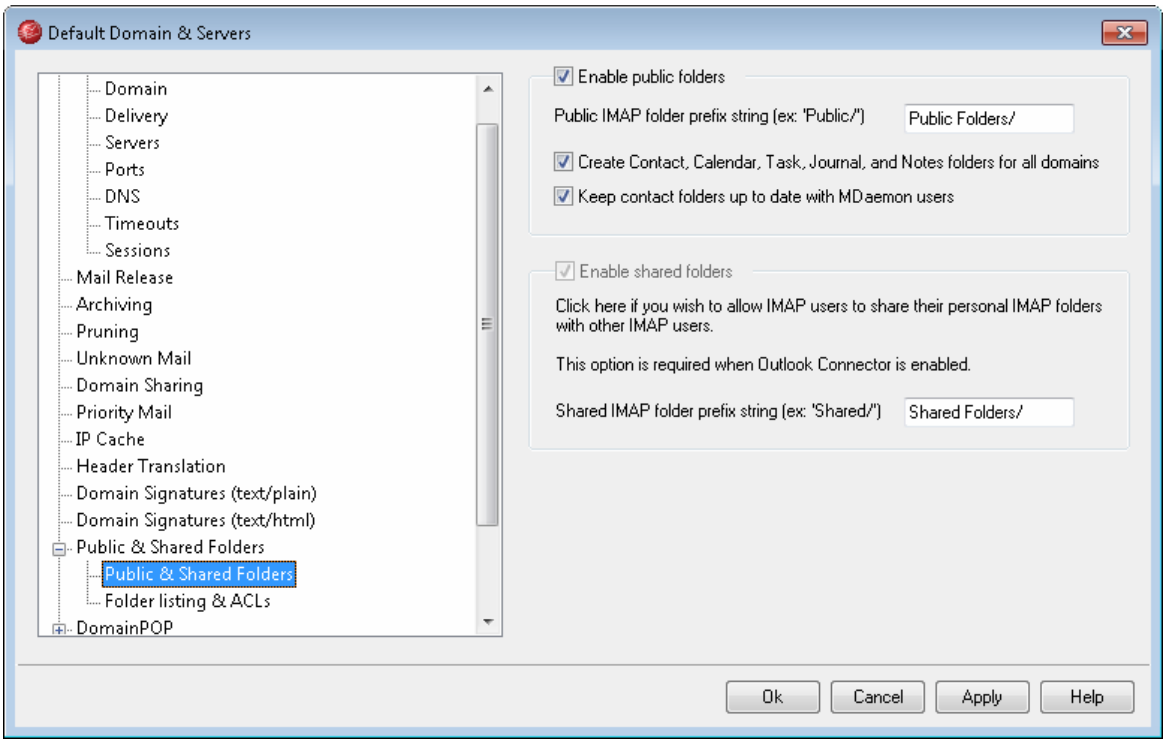
individual `\Users\..\WC\user.ini` files respectively. You can configure both default settings and customized settings, which will override the defaults. For example:

```
[Default:UserDefaults]
DocumentsFolderName=Documents
EnableDocuments=Yes

[example.com:UserDefaults]
DocumentsFolderName=Example Documents
EnableDocuments=Yes

[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableCalendar=No
EnableNotes=No
EnableTasks=No
```

**See:**

**Public & Shared Folders** 75
**Folder Listing** 77
**Access Control List** 79
**Account Editor » Shared Folders** 371

### 4.1.12.1 Public & Shared Folders




*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

To reach the Public & Shared Folders screen, click "Setup » Default Domain/Servers » Public & Shared Folders".

## Public Folders

**Enable public folders**
Click this switch if you wish to allow IMAP users to gain access to public folders. The users that can access them and the level of access granted is designated under each folder on the Folder Listing 77 screen. Clear this check box if you want to hide public folders from all users.

**Public IMAP folder prefix string (ex: 'Public/')**
Public folders are prefixed with a sequence of up to 20 characters, such as "#" or "Public Folders/". This is to help users easily distinguish public from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote public folders.

**Create Contact, Calendar, Task, Journal, and Notes folders for all domains**
Click this check box if you wish to ensure that these folders exist for all domains. Whenever a Domain 108 is added to MDaemon, these folders will be created.

**Keep contact folders up to date with MDaemon users**
If this option is enabled, MDaemon will keep the contact folders synchronized with its account list.

## Shared Folders

**Enable shared folders**
Click this switch if you wish to allow IMAP users to share access to their IMAP folders. The users who can access them and the level of access granted is designated under each folder on the Shared Folders 371 screen of the Account Editor (Accounts » Account Manager » [User Account] » Shared Folders). Clear this check box if you wish to prevent users from being able to share access to their folders, and prevent the aforementioned Shared Folders screen from appearing on the Account Editor.

When using Outlook Connector for MDaemon, this option will be unavailable. You will not be able to deactivate it because user folder sharing is required for Outlook Connector to function properly.

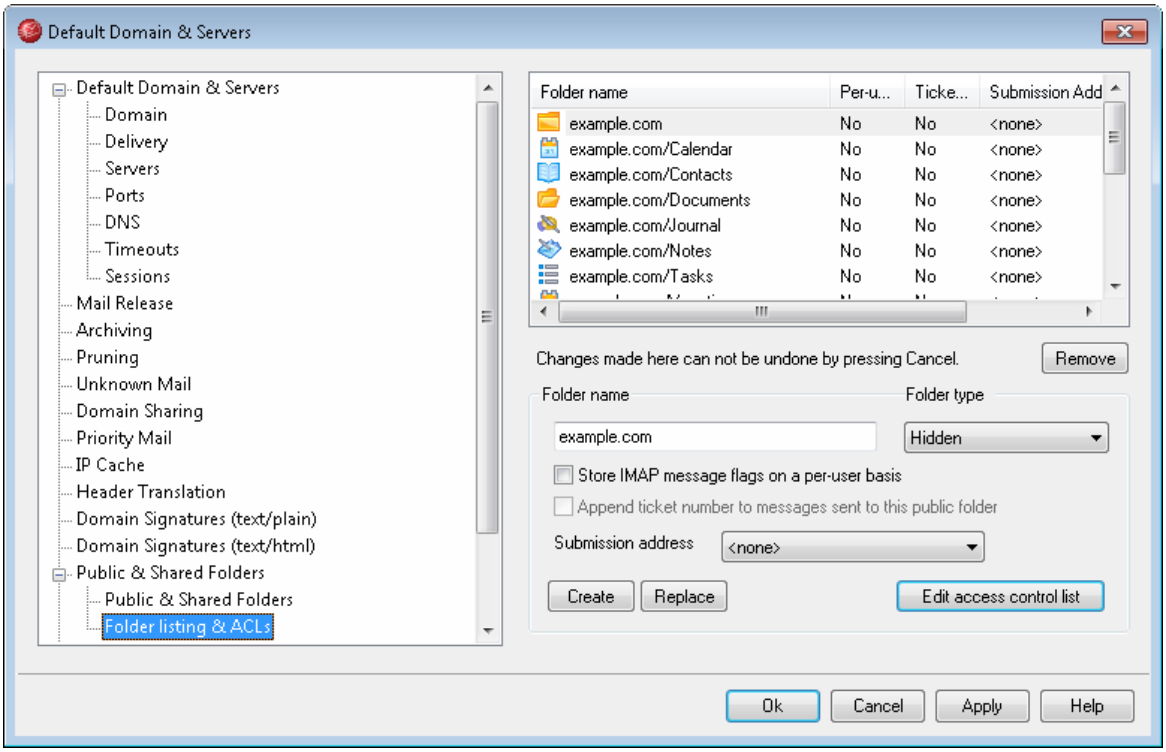
**Shared IMAP folder prefix string (ex: 'Shared/')**
Shared user folders are prefixed with a sequence of up to 20 characters, such as "Public Folders/". This is to help users easily distinguish shared from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote shared user folders.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**Folder Listing** 77
**Access Control List** 79
**Account Editor » Shared Folders** 371

### 4.1.12.2 Folder Listing




To reach the Folder Listing screen, click "Setup » Default Domain/Servers » Public & Shared Folders » Folder listing/ACLs".

**IMAP Folders**

Displayed in this area is each public IMAP folder that you have created, the *Per-user flags* setting, and the Submission Address with which each one has been associated (if any).

**Remove**

To remove a public IMAP folder from the list, select the desired folder and then click the Remove button.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### New IMAP Folder

**Folder name**
To add a new folder to the list, specify a name for it in this control, set the *Folder type*, per-user flags, and *Submission address* options, and then click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, prefix the new folder's name with the parent folder's name and a slash. For example, if the parent folder is "`My Folder`" and the new folder is "`My New Folder`," then the new subfolder name would be "`My Folder/My New Folder`". If you don't want it to be a subfolder, then name the new folder "`My New Folder`" without the prefix.

**Folder type**
Use the drop-down list to designate the type of folder this will be: Mail, Contacts, Calendar, etc.

**Store IMAP message flags on per-user basis**
Click this check box if you want the folder's message flags (read, unread, replied to, forwarded, and so on) to be set on a per-user basis instead of globally. Each user will see the status of the messages in the shared folder displayed according to their personal interaction with them. A user who hasn't read a message will see it flagged as 'unread' while a user who has read it will see the status as 'read'. If this control is disabled then all users will see the same status. So, once any user has read a message then all users will see it marked as 'read'.

**Append ticket number to messages sent to this public folder**
Use this option if you wish to configure the public folder as a message ticketing public folder. MDaemon will add the *Folder name* and a unique identifier to the subject of messages sent to the public folder's *Submission address*. Any outbound messages having this specially formatted subject will have the From address changed to the submission address of the public folder and a copy of the outbound message will be placed into a child public folder named "Replied To". In addition, any inbound messages with this specially formatted subject will be automatically redirected to the public folder, regardless of the address the message was sent to.

**Submission address**
Use this drop-down list to associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

**Create**
After specifying a folder's name and other settings, click this button to add the folder to the list.

**Replace**
If you wish to edit one of the entries, click the entry, make the desired changes to the *Folder name* or other settings, and then click *Replace*.

**Edit access control list**
Choose a folder and then click this button to open the Access Control List 79 dialog

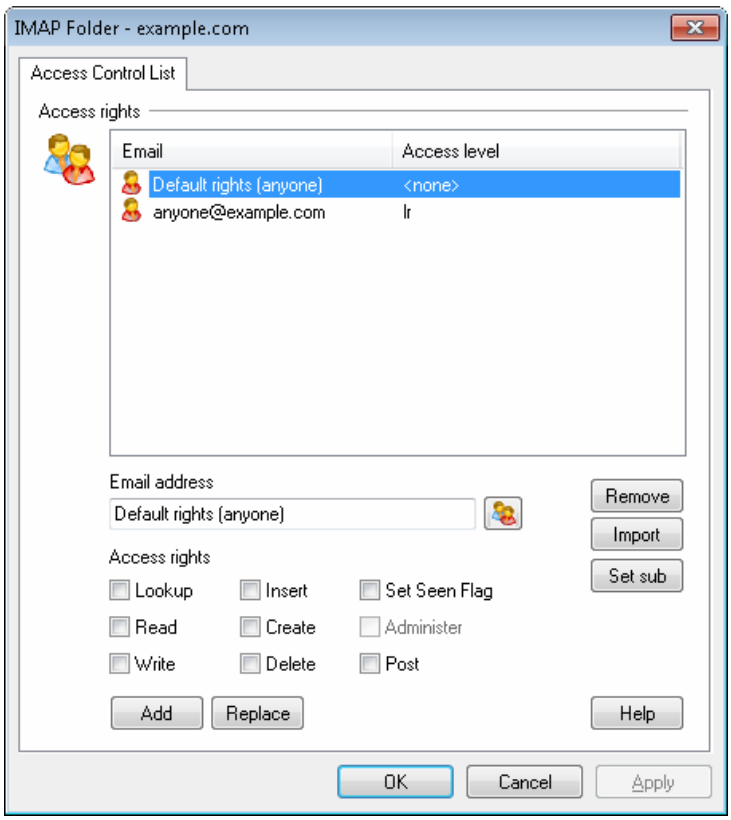
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

**See:**

**Access Control List** 79
**Public & Shared Folders** 75
**Account Editor » Shared Folders** 371

### 4.1.12.2.1 Access Control List




#### Access Rights

This area is for designating the MDaemon user accounts or groups that you wish to grant access to the associated shared folder, and for setting the access permissions for each one. You can reach this dialog from the Folder Listing screen (click "Setup » Default Domain/Servers » Public & Shared Folders » Folder listing/ ACLs"). Double-click the desired folder, or click the folder and then click *Edit access control list*, to open the Access Control List for that folder. Each entry lists the email address of the account and a one letter Access Level abbreviation for each Access Right that you grant to the user.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Email address**
Type the email address or click the Account icon to choose the MDaemon account or group that you wish to grant access to the shared folder. After designating an account or group, choose the desired Access Rights and then click *Add* to add that entry to the list.

**Remove**
To remove an entry from the Access Rights list, select the desired entry and then click *Remove*.

**Import**
With the *Import* feature you can add the members of an existing Mailing List to the list of users with Access Rights. Choose the access rights that you wish to grant to the users, click Import, and then double-click the desired list. All of the list's members will be added to the list with the rights that you set.

**Set sub**
Click *Set sub* if you wish to copy this folder's access control permissions to any subfolders it currently contains.

### Access Rights List

Choose the rights that you wish to grant to the user or group by clicking the desired options in this area and then clicking *Add* for new entries or *Replace* for existing entries.

You can grant the following Access Control Rights:

**Lookup (l)** – user can see this folder in their personal list of IMAP folders.

**Read (r)** – user can open this folder and view its contents.

**Write (w)** – user can change flags on messages in this folder.

**Insert (i)** – user can append and copy messages into this folder.

**Create (c)** – user can create subfolders within this folder.

**Delete (d)** – user can delete messages from this folder.

**Set Seen Flag (s)** – user can change the read/unread status of messages in this folder.

**Administer (a)** – user can administer the ACL for this folder.

**Post (p)** – user can send mail directly to this folder (if folder allows).

**Add**
After designating an Email Address or Group and choosing the access rights that you wish to grant, click *Add* to add the account or group to the list.

**Replace**
To modify an existing Access Rights entry, select the entry, make any desired changes to the Access Rights, and then click *Replace*.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Help**
Click *Help* to display a list of the access rights and their definitions.

Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting folder access rights to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at: http://www.rfc-editor.org/rfc/rfc2086.txt.

**See:**

**Public & Shared Folders** 75
**Folder Listing** 77

## 4.1.13 DomainPOP

Use DomainPOP Mail Collection ("Setup » Default Domain/Servers » DomainPOP") to configure MDaemon to download mail from a remote POP mailbox for redistribution to your users. This feature works by using the POP3 protocol to download all the mail found in the ISP's POP mailbox associated with the specified logon. Once collected, the messages are parsed according to the settings provided on this dialog and then placed in user mailboxes or the remote mail queue for MDaemon to deliver, just as if the messages had arrived at the server using conventional SMTP transactions.

It is important to note that messages stored in mailboxes and retrieved using the POP3 protocol will be devoid of the important routing information (sometimes called the message's "envelope") that would ordinarily be supplied had the messages been delivered using the more powerful SMTP protocol. Without this routing information, MDaemon is forced to "read" the message and examine the headers in an attempt to determine to whom the message was originally intended. This is not an exact science to say the least. Message headers are sometimes notorious for their lack of sufficient information needed to determine the intended recipient. This lack of what would seem to be a fundamental characteristic of an email message - the recipient - may seem surprising but one must keep in mind that the message was never intended to be delivered to its recipient using the POP protocol. With SMTP, the contents of the message are irrelevant since the protocol itself dictates specifically to the server, during the mail transaction, the intended recipient of the message.

In order to allow for POP retrieval and delivery of mail messages in a reliable and consistent way, MDaemon employs a powerful suite of header processing options. When MDaemon downloads a message from a remote POP source it immediately parses all the relevant headers within that message and builds a collection of potential

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

recipients. Every email address found in the headers that MDaemon inspects is included in the collection.

Once this process is complete, MDaemon's collection of recipients is divided into local and remote sets. Further, all addresses that are parsed and placed into the collection of potential recipients are processed through the Aliases 398 translator before being divided into local and remote sets. Every member of the local set (addresses with a domain that matches one of MDaemon's local domains) will receive a copy of the message. What happens to the remote set is governed by the settings in this dialog. You can elect to simply ignore these addresses, forward a summary listing of them to the postmaster, or honor them — in which case MDaemon will actually deliver a copy of the message to the remote recipient. Only under rare circumstances would the need to deliver these messages to remote recipients be warranted.

Care must be taken to prevent duplicate messages or endlessly looping mail delivery cycles. A common problem that results from the loss of the SMTP envelope manifests itself with mailing list mail. Typically, messages distributed by a mailing list do not contain within the message body any reference to the addresses of the recipients. Rather, the list engine simply inserts the name of the mailing list into the `TO:` field. This presents an immediate problem: if the `TO:` field contains the name of the mailing list then the potential exists for MDaemon to download this message, parse the `TO:` field (which will yield the name of the mailing list), and then dispatch the message right back to the same list. This would in turn deliver another copy of the same message back to the POP mailbox from which MDaemon downloaded the original message — thus starting the whole cycle over again. To cope with such problems mail administrators must take care to use the tools and settings that MDaemon provides to either delete mailing list mail or perhaps alias it in such a way that it will be delivered to the proper local recipient(s). You could also utilize the Routing Rules or Content Filters to deliver the message to the correct recipient(s).

Additional concerns when employing this sort of mail collection scheme revolve around the issue of unwanted message duplication. It is very easy for mail that is delivered to the ISP's POP mailbox using SMTP to generate unwanted duplicates, once it has been collected using DomainPOP. For example, suppose a message is sent to someone at your domain and a carbon copy is sent to another person at the same domain. In this situation, SMTP will deliver **two** copies of the same message to your ISP's mailbox — one for each recipient. Each of the two message files will contain references to **both** recipients — one in the `TO:` field and the other in the `CC:` field. MDaemon will collect each of these two identical message files and parse both addresses from each of them. This would result in both recipients receiving one unwanted duplicate message. To guard against this sort of duplication MDaemon uses a control which allows you to specify a header that MDaemon will use to check for duplication. The `Message-ID` field is ideal for this. In the above example, both messages are identical and will therefore contain the same `Message-ID` field value. MDaemon can use this value to identify and remove the second message during the download stage before it can be parsed for address information.

As a final measure guarding against duplicate messages and endless looping delivery cycles, MDaemon employs a means for detecting how many trips or "hops" a message has made through the transport system. Each time an SMTP mail server processes a message it "stamps" the message with a "Received" header. MDaemon counts all such headers when it encounters a message for the first time. If the total number of mail servers exceeds a specified value, it is likely the message is caught in a delivery loop

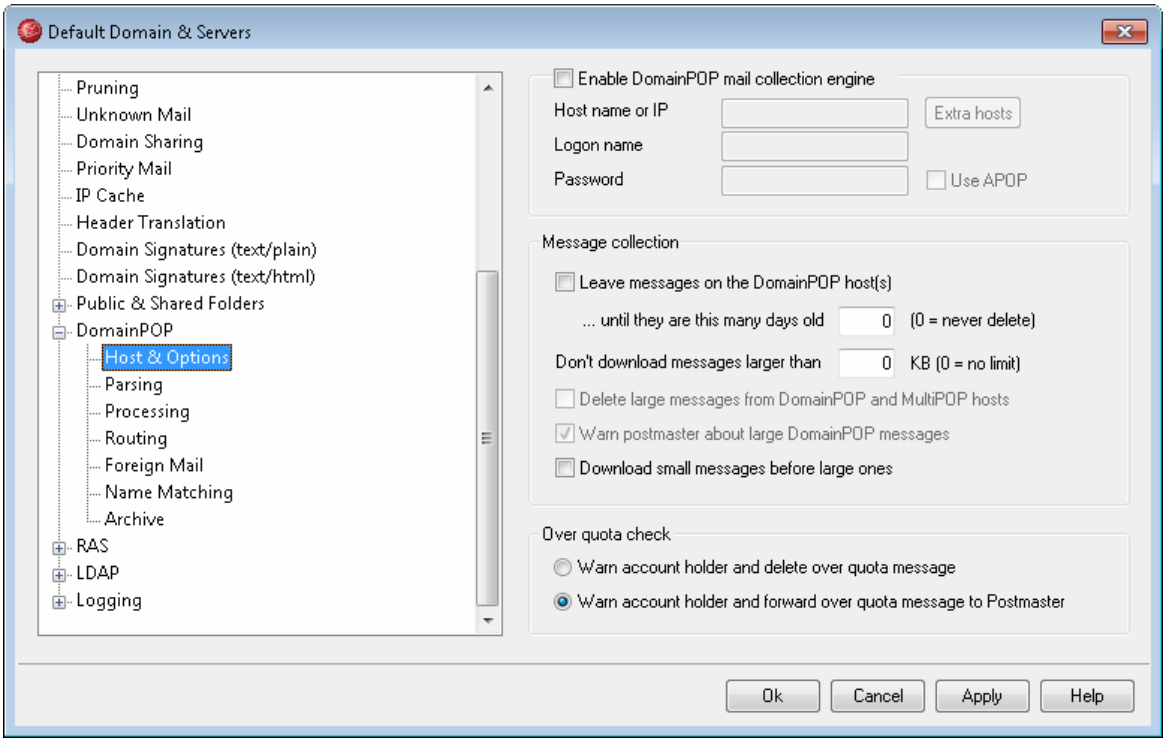
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

and should be taken out of the mail stream and moved to the bad message directory. This value can be configured through the Timeouts 53 screen of the Default Domain editor.

**See:**

**Content Filters** 210
**Mailing Lists** 430

### 4.1.13.1 Host & Options




#### DomainPOP Host Properties

**Enable DomainPOP mail collection engine**
If selected, MDaemon will use the setting provided on this screen to collect mail from a DomainPOP mail host for local redistribution.

**Host name or IP**
Enter your DomainPOP host's domain name or IP address here.

**Extra hosts**
Click this button to open the `DpopXtra.dat` file, on which you can designate extra hosts from which to collect DomainPOP mail. See the contents of that file for more information.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Logon name**
Enter your login of the POP account used by DomainPOP.

**Password**
Enter the POP or APOP account's password here.

**Use APOP**
Click this box if you wish to use the APOP command and CRAM-MD5 authentication when retrieving your mail. This makes it possible to authenticate yourself without having to send clear text passwords.

## Message Collection

**Leave messages on the DomainPOP host(s)**
If selected, MDaemon will download but not remove the messages from your DomainPOP mail host.

**...until they are this many days old (0=never delete)**
This is the number of days that a message can remain on the DomainPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

Some hosts may limit the amount time that you are allowed to store messages in your mailbox.

**Don't download messages larger than [XX] KB (0 = no limit)**
Messages greater than or equal to this size will not be downloaded from your DomainPOP mail host. Enter "0" if you want MDaemon to download messages no matter the size.

**Delete large messages from DomainPOP and MultiPOP hosts**
Enable this option and MDaemon will delete messages that exceed the size designated above. The messages will simply be removed from the DomainPOP and MultiPOP mail hosts and will not be downloaded.

**Warn postmaster about large DomainPOP messages**
Check this option and MDaemon will send a warning to the postmaster whenever a large message is discovered in the DomainPOP mailbox.

**Download small messages before large ones**
Enable this checkbox if you want the message downloading order to be based on size — beginning with the smallest and proceeding to the largest.

This option retrieves smaller messages quicker but requires a larger amount of internal sorting and processing.

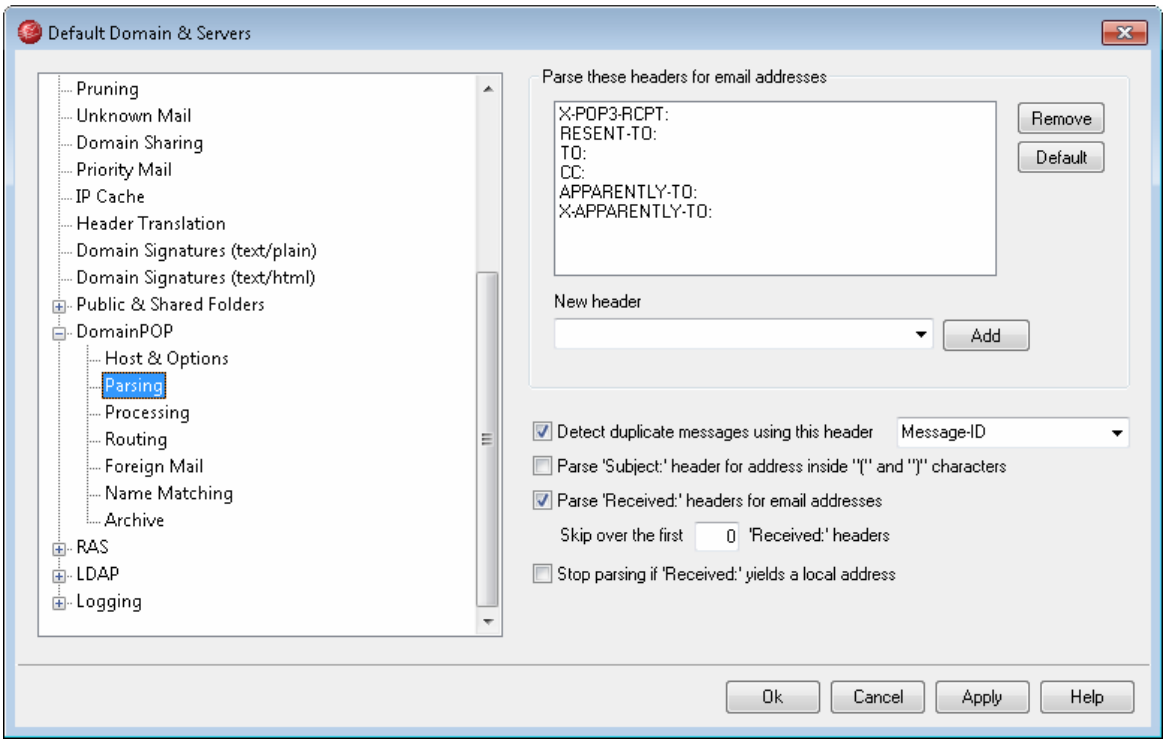
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Over Quota Check

**Warn account holder and delete over quota message**
When this option is chosen and a message is collected for an account that is over its quota (designated on the Quotas 366 screen of the account editor), MDaemon will delete the message and then send a message to the account holder stating that the account is over its limit.

**Warn account holder and forward over quota message to Postmaster**
When this option is chosen and a message is collected for an account that is over its quota, MDaemon will forward the message to the Postmaster and send a warning to the user letting him or her know that the account is over its limit.

## 4.1.13.2 Parsing




### Parse these headers for email addresses

This area lists the headers that MDaemon will parse in an attempt to extract addresses. Every header listed here is checked for addresses.

**Remove**
This button will remove the selected entries from the header list.

**Default**
This button will clear the current contents of the header list and add MDaemon's default list of headers. The default headers are typically sufficient to extract all

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

addresses from the message.

**New header**
Enter the header you wish to add to the header list.

**Add**
After specifying a header in the *New header* option, click this button to add it to the list.

**Delete duplicated messages using this header**
If this option is selected MDaemon will remember the value of the specified header and will not process additional messages collected in the same processing cycle which contain an identical value. The `Message-ID` header is the default header used by this option.

**Parse "subject:" header for address inside "(" and ")" characters**
When this is selected and MDaemon finds an address contained in "( )" in the "Subject:" header of a message, this address will be added to the message's list of recipients along with any other parsed addresses.

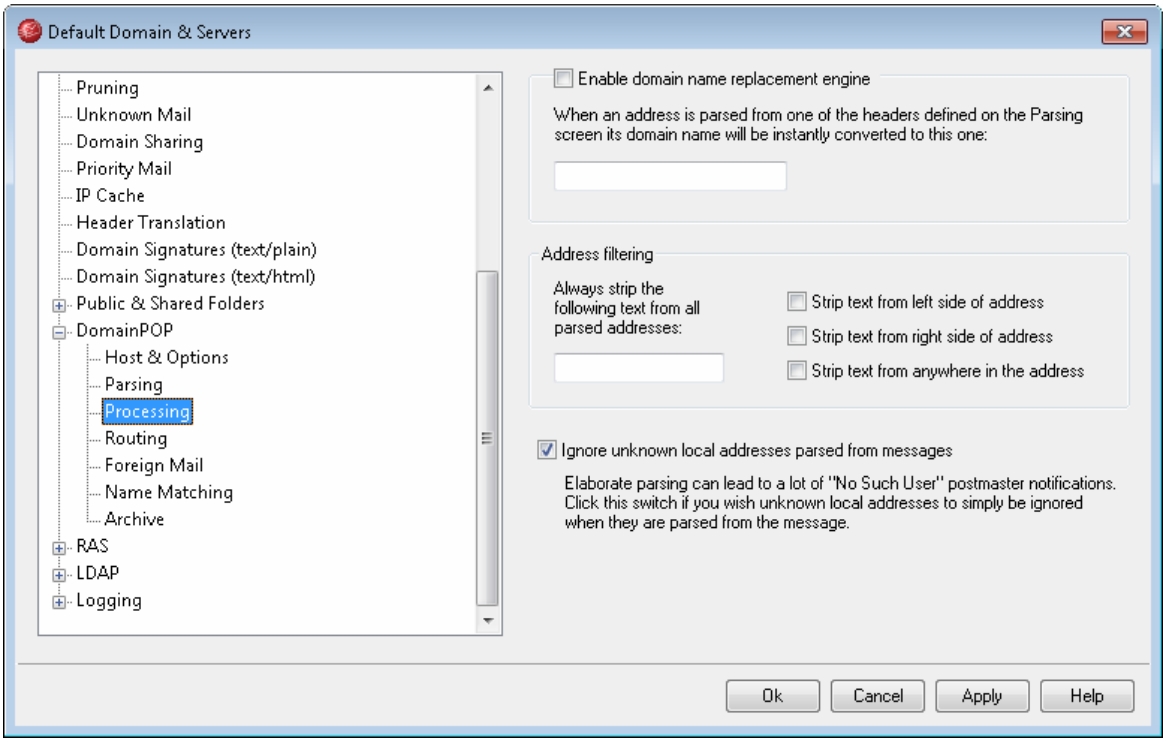
**Parse "Received" headers for email addresses**
It is possible to store the recipient information ordinarily found only within the message's envelope in the "Received" message headers. This makes it possible for parsers of the mail message to be able to glean the actual recipient address by merely inspecting the Received headers later. Click this checkbox if you wish to parse valid addresses from all of the "received" headers found within the mail message.

**Skip over the first xx "received" headers**
In some server configurations you may wish to parse Received headers but need to skip the first few of them. This setting allows you to enter the number of "Received" headers that MD will skip over before beginning its parsing.

**Stop parsing if "Received" yields a valid local address**
If while parsing a "received" header MDaemon detects a valid local address, this switch will cause all further parsing to stop and MDaemon will not search the message for more potential delivery addresses.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.13.3 Processing




#### Domain Name Replacement

**Enable domain name replacement engine**
This option can be used to reduce the number of aliases your site might require. When a message is downloaded, all domain names in all addresses parsed from that message will be converted to the domain name specified here.

#### Address Filtering

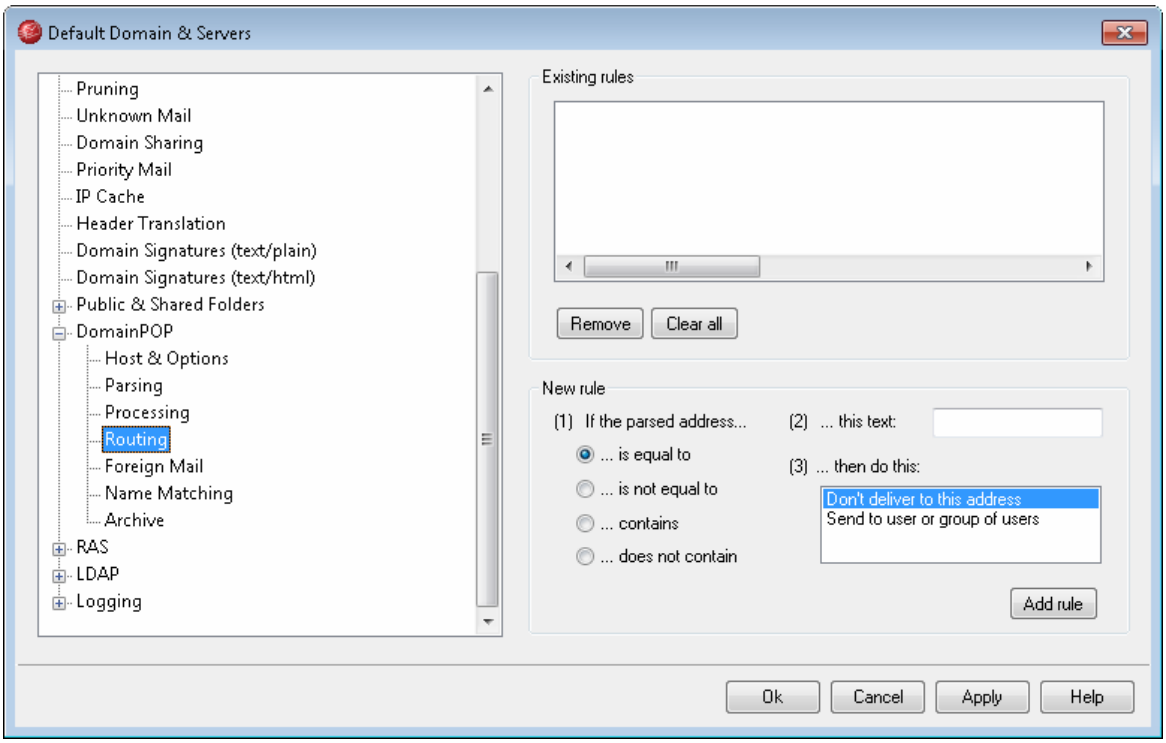
**Always strip the following text from all parsed addresses**
Some hosts will stamp each message with a line that indicates who the recipient of the message should be, along with a bit of routing information appended to the address on either the left or right side. This stamp would be perfect to use for parsing the recipient address except that the additional routing information makes this impossible without a lot of account aliasing. Rather than do all that you can simply specify the value of this appended text in the edit control associated with this feature and MDaemon will strip any occurrence of this text from all addresses that it parses.

**Ignore unknown local addresses parsed from messages**
As mentioned above, the Domain Name Replacement feature will alter the domain name in all email addresses parsed from a message, converting it into the one you specify on this screen. This could create some addresses that do not have a corresponding account your server. Because the domain name but not the mailbox

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

would be valid, MDaemon would consider such addresses unknown local users. Such mail typically generates a "No Such User" message. Check this box if you wish to prevent the Domain Name Replacement Engine from causing these messages to be generated.

### 4.1.13.4 Routing




#### Existing Rules

This list shows you the rules that you have created and will be applied to your messages.

**Remove**
Select a rule from the list and then click this button to delete it.

**Clear all**
This button removes all existing rules.

#### New Rule

**(1) If the parsed address...**

**Is equal to, is not equal to, contains, does not contain**
This is the type of comparison that will be made when an address is compared to this routing rule. MDaemon will search each address for the text contained in the *"...this text*" option below and then proceed based upon this option's setting — does the address's complete text match exactly, not match exactly, contain the text, or

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

not contain it at all?

**(2) ...this text:**
Enter the text that you want MDaemon to search for when scanning the addresses.

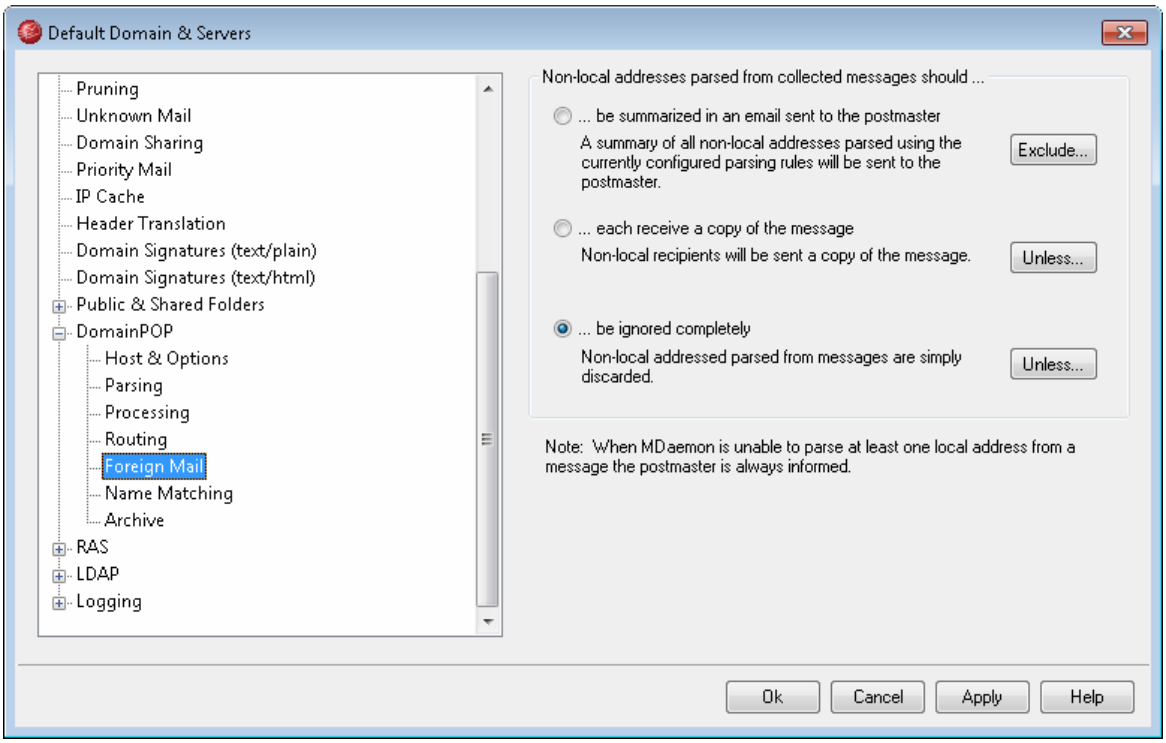
**(3) ...then do this:**
This option lists the available actions that can be performed if the result of the rule is true. You can choose from the following actions:

*Don't deliver to this address* - Selecting this action will prevent the message from being delivered to the specified address.

*Send to user or group of users* - Selecting this action will open dialog on which you can designate a list of email addresses that should receive a copy of the message being processed.

**Add rule**
After setting the new rule's parameters, click *Add rule* to add it to the list of rules.

### 4.1.13.5 Foreign Mail




**Non-local addresses parsed from collected messages should...**

**...be summarized in an email sent to the postmaster**
If this option is selected MDaemon will send a single copy of the message to the postmaster along with a summary of the non-local addresses that the parsing

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

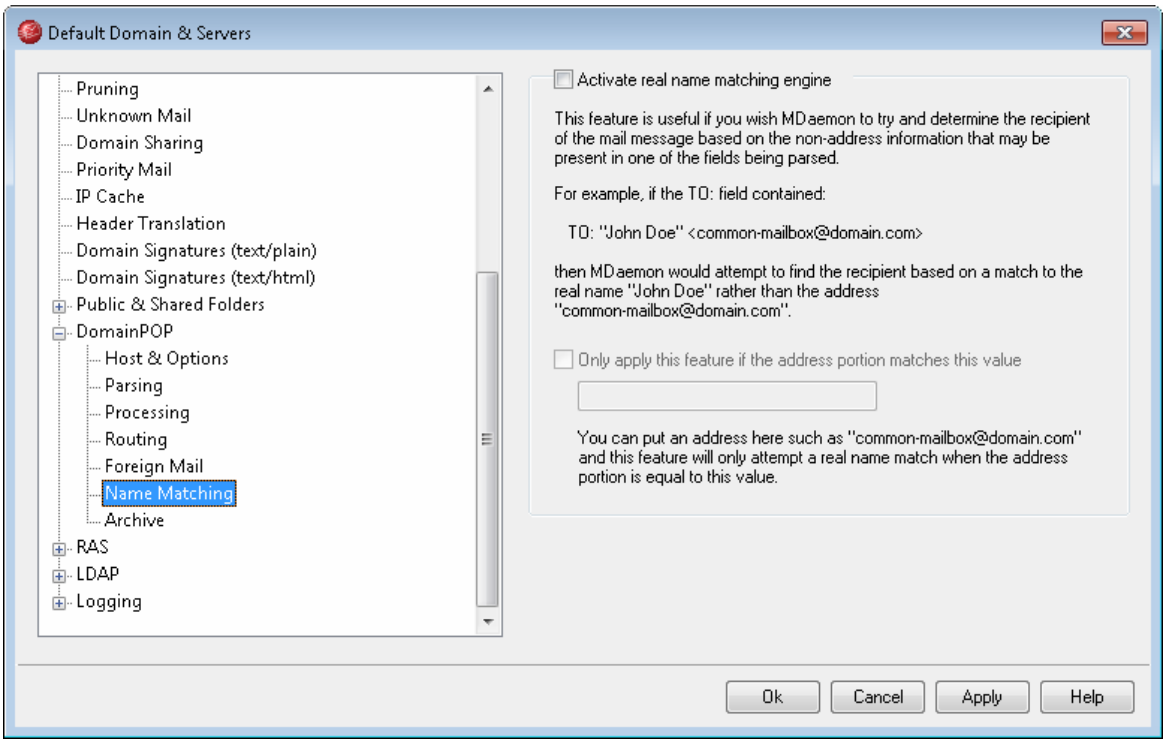
engine extracted using the current set of headers and parsing rules.

**...each receive a copy of the message**
If this option is selected MDaemon will deliver a copy of the message to any non-local recipient that it finds within the inspected headers.

**...be ignored completely**
If this option is selected MDaemon will remove from the recipient list any address that is non-local. It will be as if MDaemon never parsed remote addresses from the original downloaded message.

The *Exclude...* and *Unless...* buttons allow you to define addresses that will be treated as exceptions to the the selected option.

### 4.1.13.6 Name Matching




The Name Matching feature is only active in conjunction with the DomainPOP Mail Collection engine. If you wish to use this feature, you must make sure that you have DomainPOP enabled. DomainPOP can be reached from the "Setup » Default Domain/Servers » DomainPOP" menu selection.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Real Name Matching Engine

**Activate real name matching engine**
This feature allows MDaemon to determine who should receive a DomainPOP collected message based not upon the parsed email address but upon the text included with the address. This is typically the recipient's real name.

For example, a message's TO header might read:

```
TO: "Michael Mason" <user01@example.com>
```

or

```
TO: Michael Mason <user01@example.com>
```

Name Matching ignores the "user01@example.com" portion of the address. It instead extracts the "Michael Mason" portion and checks to see if this is an MDaemon user. If a match is found to an account's real name then that account's local email address is used for delivery purposes. If no match is made then MDaemon reverts to delivering the message to the email address parsed from the data (user01@example.com in this example).

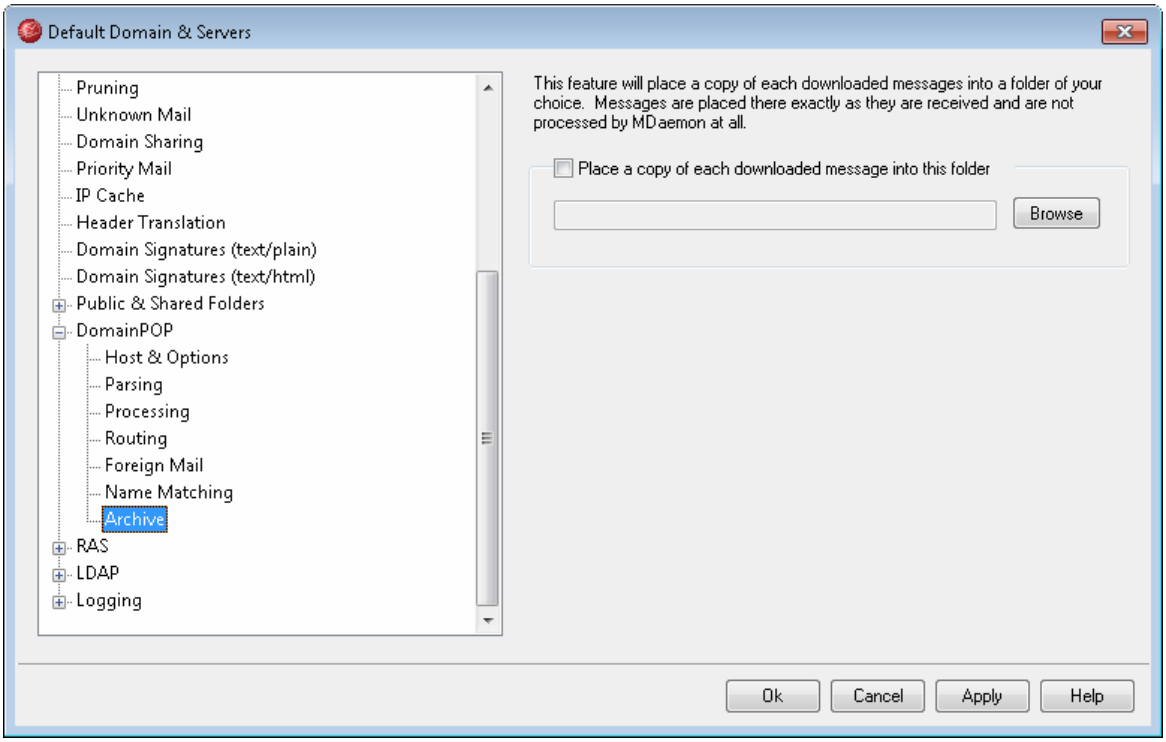
The real name portion of the address may not contain a comma, semi-colon, or colon character.

**Only apply this feature if the address portion matches this value**
This option allows you to specify an email address that must be present in the extracted data in order for the real name matching process to proceed. This allows you a measure of control over when the Name Matching feature will be employed. For example, you can specify an address such as "user01@example.com" and then only addresses matching this value will be candidates for Name Matching.

Suppose you specify "user01@example.com" in this option. This means that "**TO: 'Michael Mason' <user01@example.com>**" will be a candidate for Name Matching while "**TO: 'Michael Mason' <user02@example.com>** will not.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.13.7 Archive




**Archive**

**Place a copy of each downloaded message into this folder**
This is a safety feature to ensure that you don't lose any mail due to unforeseen parsing or other errors that might occur when downloading mail in bulk quantities. Check this box if you wish to save a copy of each downloaded message into the folder that you specify. These copies are placed in the folder exactly as they are received and are not processed by MDaemon at all.

## 4.1.14 RAS Dialup Settings

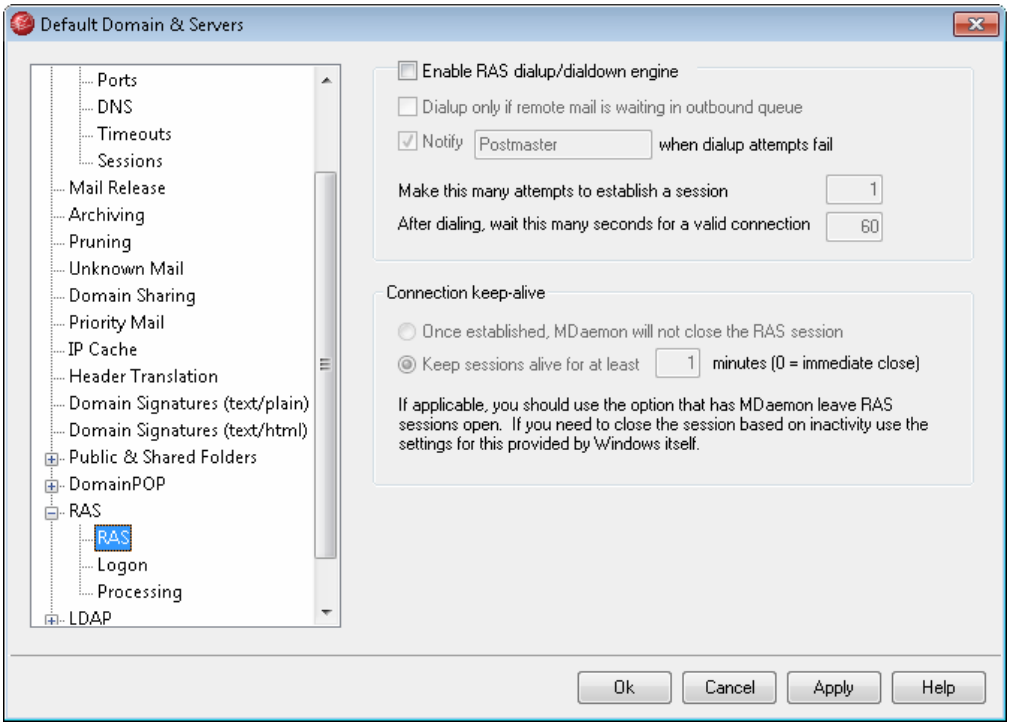
Click the "Setup » Default Domain/Servers » RAS" menu selection to configure your RAS Dialup settings. This dialog will only be available if you have Remote Access Services installed on your system. It is used by MDaemon when you need to dial up your ISP just prior to a Remote Mail processing event.

The RAS Dialup contains the following three screens:

- **RAS** 93
- **Logon** 94
- **Processing** 95

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.14.1 RAS




**Enable RAS dialup/dialdown engine**
When this option is enabled, MDaemon will use the settings specified here to make a connection to a remote host before sending or receiving remote mail.

**Dialup only if remote mail is waiting in outbound queue**
When this box is checked, MDaemon will not dial the ISP unless there is remote mail waiting in the Remote queue. This may be beneficial in some circumstances but be aware that if MDaemon does not dial up then it cannot do any mail **collecting** either (unless it is delivered across the local LAN).

**Notify [address] when dialup attempts fail**
When selected, MDaemon will send a message to the specified address when a dialup event fails because of some error.

**Make this many attempts to establish a session**
MDaemon will attempt to connect to the remote host this many times before giving up.

**After dialing, wait this many seconds for a valid connection**
This value determines how long MDaemon will wait for the remote computer to answer and complete the RAS connection.

#### Connection Keep-alive

**Once established, MDaemon will not close the RAS session**
By default, MDaemon will shut down a created connection immediately after all mail

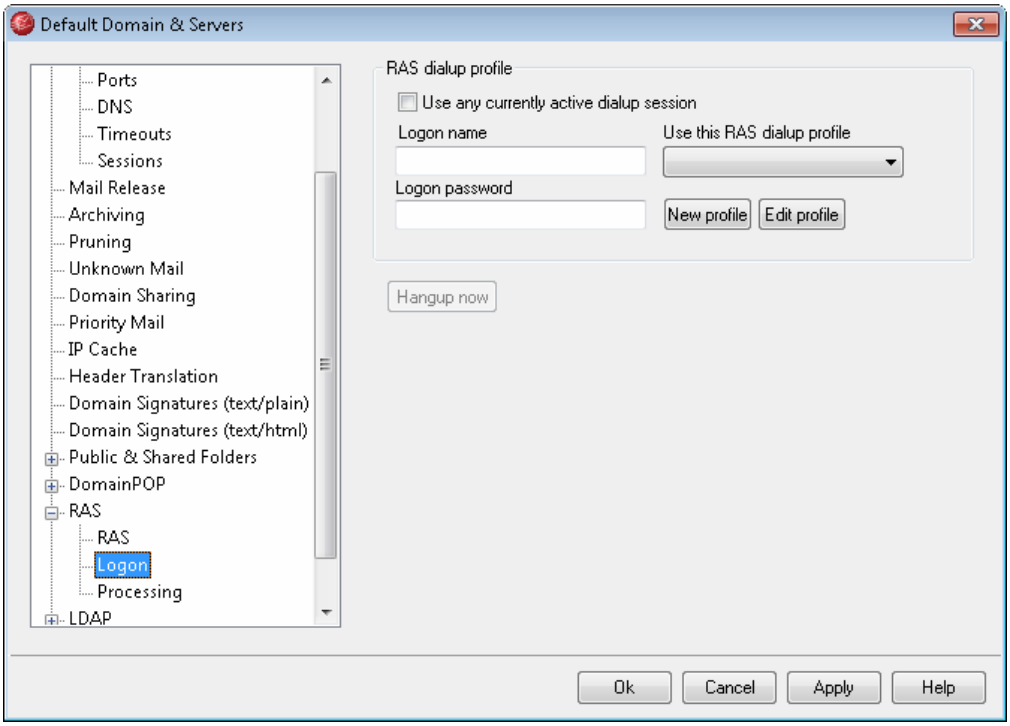
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

transactions have been completed and the session is no longer in use. Selecting this option will cause the connection to remain open even after all transactions have been completed.

MDaemon will never close a connection that it did not create.

**Keep sessions alive for at least xx minutes**
If enabled, this option will cause an MDaemon created RAS session to remain open for at least the number of minutes specified or until all mail transactions have been completed, whichever is greater.

### 4.1.14.2 Logon




#### RAS Dialup Profile

**Use any currently active dialup session**
Click this checkbox if you want MDaemon to be able to utilize other connection profiles when it detects that one is active. Whenever it is time to dialup, MDaemon will first check to see if there is an active connection that it can use rather than dialing.

**Logon name**
The value specified here is the user identification or login name that will be passed to the remote host during the authentication process.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Logon Password**
The value specified here is the password that will be passed to the remote host during the authentication process.

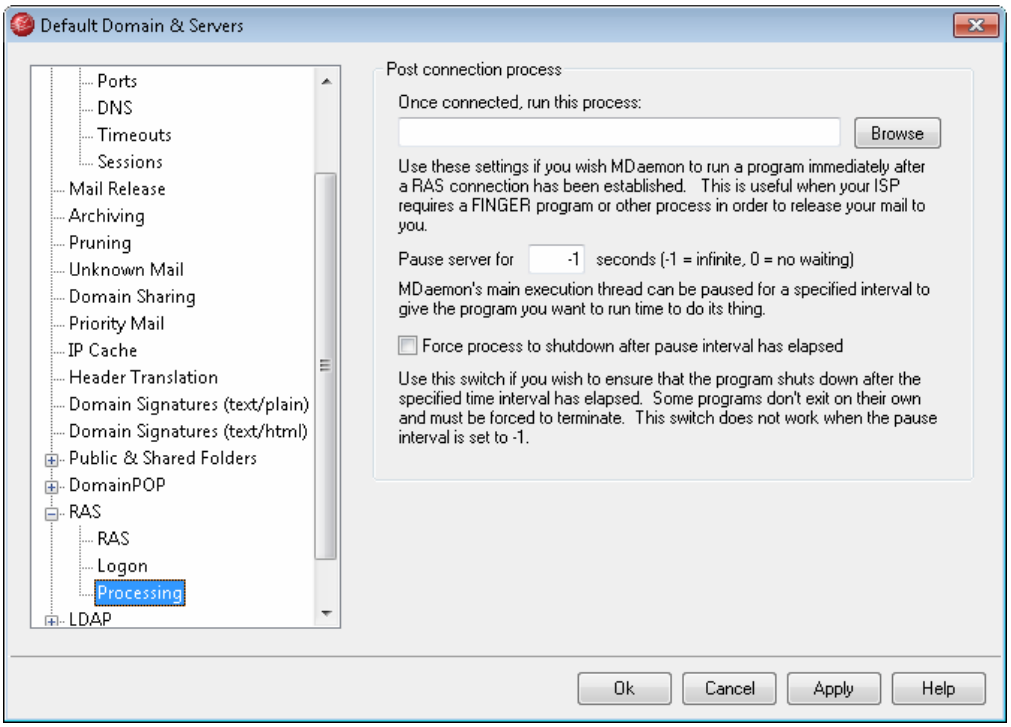
**Use this RAS dialup profile**
This drop-down list box allows you to select a session profile that has been previously defined through windows Dialup Networking or Remote Access Services Setup.

**New profile**
Click this button to create a new Dialup Networking or Remote Access Services profile.

**Edit profile**
Click this button to edit the currently selected Dialup Networking or Remote Access Services profile.

**Hangup now**
This button will close the connection to the ISP. This button is active only when MDaemon initiated the RAS session.

### 4.1.14.3 Processing




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Post Connection Process

**Once connected, run this process**
If a program is specified here, MDaemon will spawn a thread and execute the process. This is useful for those who require `Finger` or some other program to unlock the ISP's mailbox.

**Pause server for xx seconds (-1 = infinite, 0=no waiting)**
If the *Once Connected, Run This Process* control contains a valid entry then the server will pause its operations for the number of minutes specified here while it waits for the executing process to return. Entering "-1" will cause the server to wait indefinitely for the process to return.

**Force process to shutdown after pause interval has elapsed**
Sometimes the program you need to run may not exit once it has run its course; some programs require user intervention in order to close them down. This is not acceptable when the software must run unattended. If this switch is selected MDaemon will force the process thread to terminate once the number of seconds specified in *Pause Server For XX Seconds* has elapsed. This function does not work when the server is configured to wait indefinitely for the process to return.

## 4.1.15 LDAP/Address Book Options

MDaemon supports Lightweight Directory Access Protocol (LDAP) functionality. Click "`Setup » Default Domain/Servers » LDAP`" to reach the LDAP screen used for configuring MDaemon to keep your LDAP server up to date on all of its user accounts. MDaemon can maintain an accurate and continuously up to date LDAP database of users by communicating with your LDAP server each time an MDaemon account is added or removed. This makes it possible for users with mail clients that support LDAP to "share" a global address book that will contain entries for all of your MDaemon users as well as any other contacts that you include.

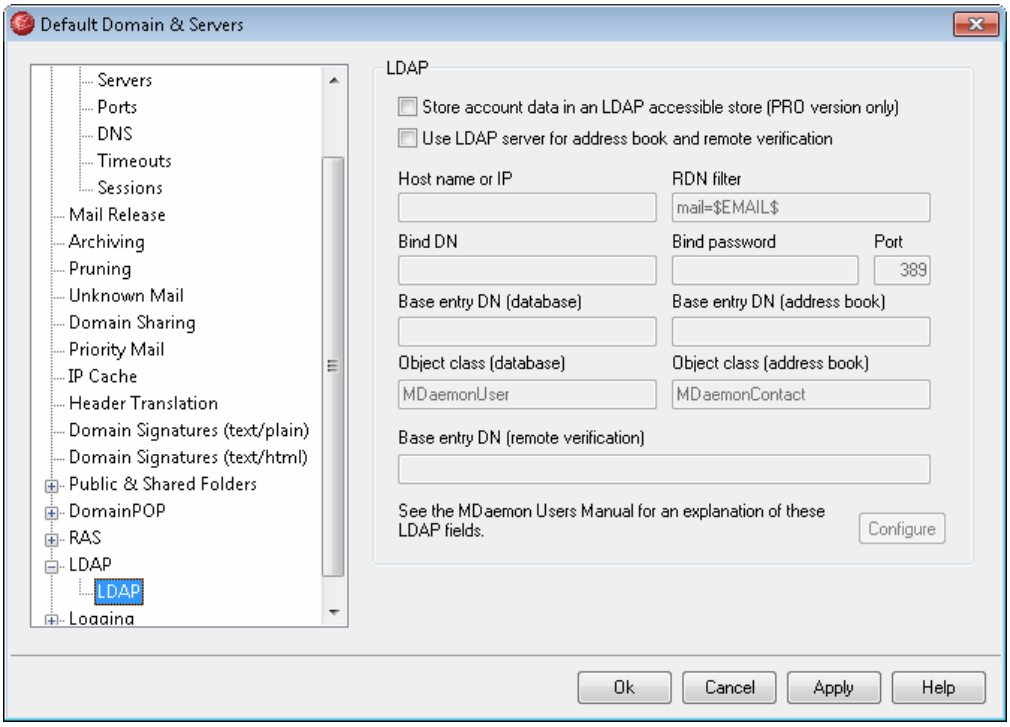
You can also use your LDAP server as the MDaemon user database rather than its local `USERLIST.DAT` system or an ODBC compliant database. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

**See:**

**LDAP** 97
**Account Database Options** 411

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.1.15.1 LDAP




#### LDAP

**Store account data in an LDAP accessible store (PRO version only)**
Click this check box if you want MDaemon to use your LDAP server as the MDaemon user database rather than ODBC or its local `USERLIST.DAT` system. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

**Use LDAP server for address book and remote verification**
If you are using ODBC or the default `USERLIST.DAT` method of maintaining your account database rather than the LDAP server method, you can still keep an LDAP server up to date with all of your users' names, email addresses, and aliases by enabling this checkbox. Thus, you can still keep an LDAP server up to date for use as a global address book system for users of email clients that contain support for LDAP address books.

This will maintain a database of your mailboxes, aliases, and mailing lists that your remote backup servers can query for remote verification of address information. See *Base entry DN (remote verification)* below for more information.

#### LDAP Server Properties

**Host name or IP**
Enter the host name or IP address of your LDAP server here.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**RDN filter**
This control is used to generate the RDN for each user's LDAP entry. The relative distinguished name (RDN) is the leftmost component in each entry's distinguished name (DN). For all peer entries (those sharing a common immediate parent) the RDN must be unique, therefore we suggest using each user's email address as their RDN to avoid possible conflicts. Using the $EMAIL$ macro as the value of the attribute in this control (i.e. `mail=$EMAIL$`) will cause it to be replaced by the user's email address when their LDAP entry is created. The user's DN will be comprised of the RDN plus the *Base entry DN* below.

**Bind DN**
Enter the DN of the entry to which you have granted administrative access to your LDAP server so that MDaemon can add and modify your MDaemon user entries. This is the DN used for authentication in the bind operation.

**Bind Password**
This password will be passed to your LDAP server along with the *Bind DN* value for authentication.

**Port**
Specify the port that your LDAP server is monitoring. MDaemon will use this port when posting account information to it.

**Base entry DN (database)**
Enter the base entry (root DN) that will be used in all of your MDaemon user entries when you are using the LDAP server as your user database rather than the `USERLIST.DAT` file. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

**Base entry DN (address book)**
When mirroring account information to an LDAP database address book, enter the base entry (root DN) that will be used in all of your MDaemon user address book entries. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

**Object class (database)**
Specify the object class to which each MDaemon user's user database entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

**Object class (address book)**
Specify the object class to which each MDaemon user's LDAP address book entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

**Base entry DN (remote verification)**
One common problem with domain gateways and backup servers is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if a message comes to example.com's backup server for `user1@example.com` then the backup server has no way of knowing whether or not there is actually a mailbox, alias, or mailing list at example.com for "`user1`". Thus

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the backup server has no choice but to accept all of the messages. MDaemon contains a method for verifying these addresses and solving this problem. By specifying a Base entry DN that will be used for all mailboxes, aliases, and mailing lists, your LDAP server can be kept up to date with all of this information. Then, your backup server can simply query your LDAP server each time a message arrives for your domain and verify whether or not the recipient's address is valid. If it isn't then the message will be rejected.

**Configure**
Click this button to open the `LDAP.dat` configuration file in a text editor. It is used for designating the LDAP attribute names that will correspond to each MDaemon account field.

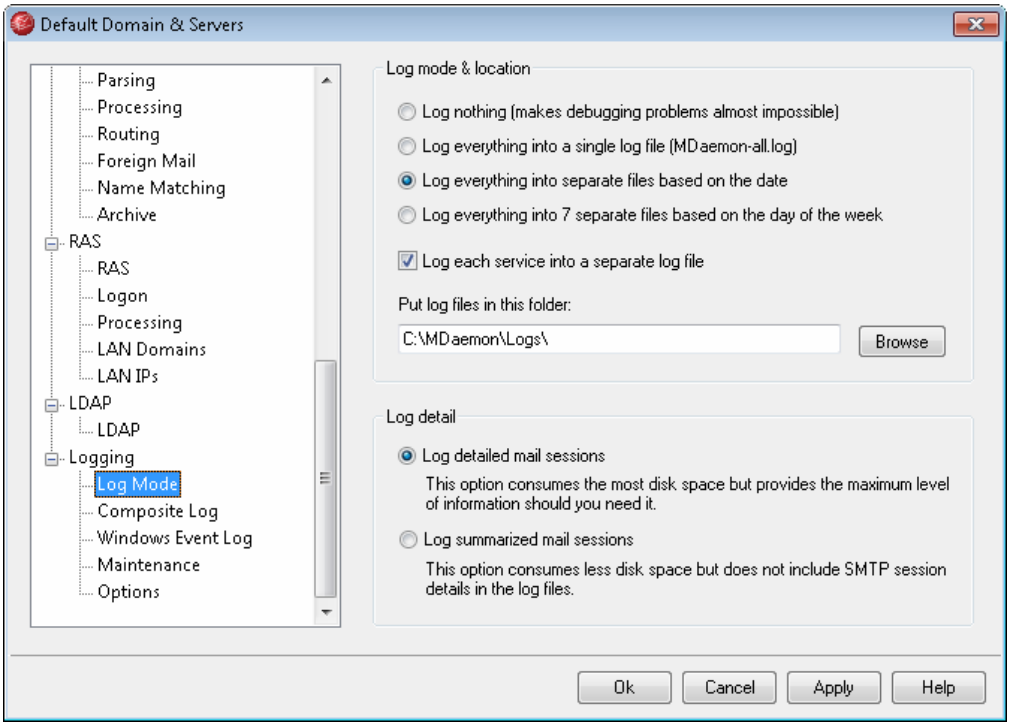
**See:**

**Account Database Options** 411

## 4.1.16 Logging

Click the "Setup » Default Domain/Servers » Logging" menu selection to configure your logging settings. Logging is a useful tool for diagnosing problems and seeing what the server has been doing while unattended.

### 4.1.16.1 Log Mode




*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

There are several options on the Preferences dialog governing the amount of log data that may be displayed in the Event Tracking pane of MDaemon's main interface. For more information, see Preferences » GUI 193.

## Log Mode & Location

**Log nothing**
Choosing this option will deactivate all logging. The log files will still be created, but no logging data will be written to them.

We do not recommend using this option. Without logs it can be extremely difficult, if not impossible, to diagnose or debug any potential email-related problems you may encounter.

**Log everything into a separate log file (MDaemon-all.log)**
Choose this option if you wish to log everything into a single, separate file named `MDaemon-all.log`.

**Log everything into separate files based on the date**
If this option is selected then a separate log file will be generated each day. The name of the file will correspond to the date it was created.

**Log everything into 7 separate files based on the day of the week**
If this option is selected, a separate log file will be generated for each day of the week. The name of the log file will correspond to the day of the week on which it was created.

**Log each service into a separate log file**
Click this checkbox to cause MDaemon to maintain separate logs by service rather than in a single file. For example, with this switch set MDaemon will log SMTP activity in the `MDaemon-SMTP.log` file and IMAP activity in the `MDaemon-IMAP.log` file. When running a Configuration Session or Terminal Services instance of the MDaemon interface, this option must be selected in order for the tabs on the interface to display the logged information.

**Put log files in this folder:**
Use this option if you wish to designate a specific folder path for your log files.

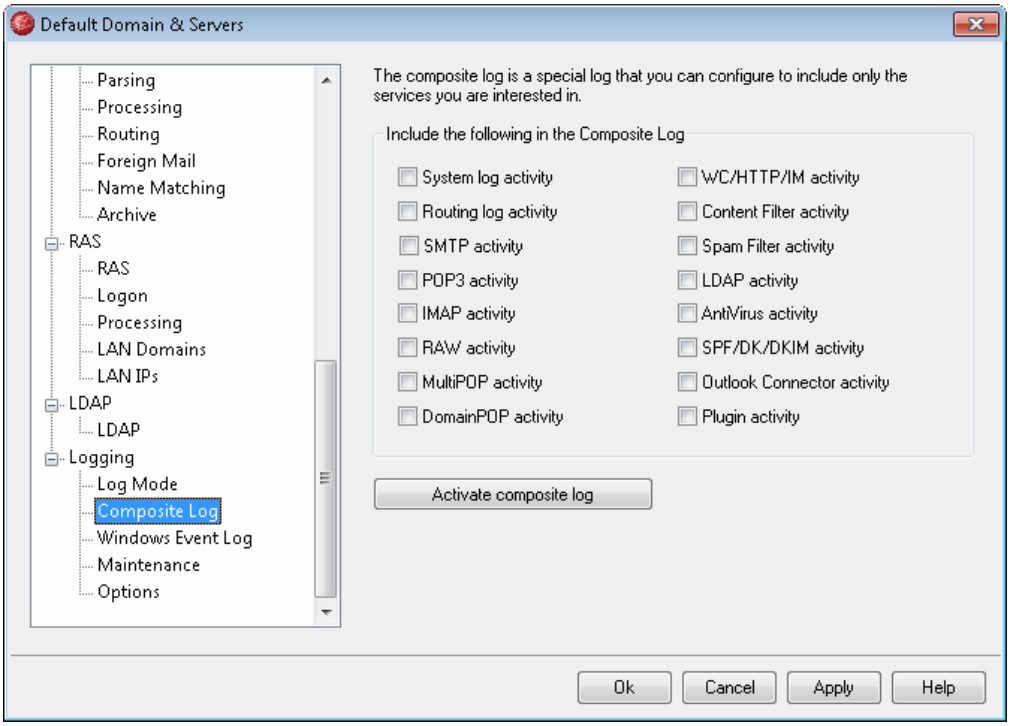
## Log Detail

**Log detailed mail sessions**
A complete transcript of each mail transaction session will be copied to the log file when this option is active.

**Log summarized mail sessions**
The option causes a summarized transcript of each mail transaction session to be copied to the log file.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.1.16.2 Composite Log




#### Composite log

**Include the following in the Composite Log**

Located on the Windows menu of MDaemon's menu bar is a Composite Log View option. Clicking that option will add a window to MDaemon's main display that will combine the information displayed on one or more of the Event Tracker's tabs. Use the controls in this section to designate which tabs' information to combine in that window. The information contained on the following tabs can be combined:

**System**—Displays MDaemon's system activity such as initializing services and enabling/disabling any of MDaemon's various servers.

**Routing**—Displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

**SMTP**—All send/receive session activity using the SMTP protocol is displayed.

**POP3**—When users collect email from MDaemon using the POP3 protocol, that activity is logged.

**IMAP**—Mail sessions using the IMAP protocol are logged.

**RAW**—RAW or system generated message activity is logged.

**MultiPOP**—Displays MDaemon's MultiPOP mail collection activities.

**DomainPOP**—Displays MDaemon's DomainPOP activity.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**WorldClient/HTTP/IM**—Displays all WorldClient activity and ComAgent instant messages activity.

**Content Filter**—MDaemon's Content Filter operations are listed.

**Spam Filter**—Displays all Spam Filtering activity.

**LDAP**—Displays LDAP activity.

**AntiVirus**—AntiVirus operations are display in the composite view.

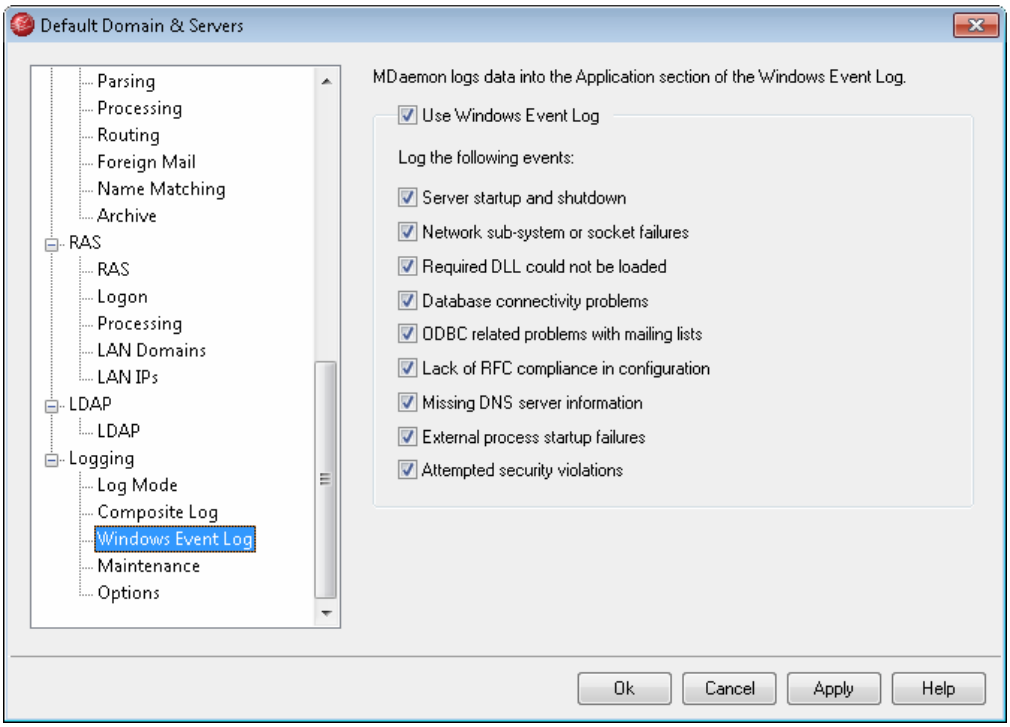
**SPF/DK/DKIM**—Displays all Sender Policy Framework and DomainKeys activity.

**Outlook Connector**—Displays all Outlook Connector activity.

**Plugin activity**—Logs MDaemon plugin activities to the composite log.

**Activate composite log**
Click this button to launch the composite log window in MDaemon's main interface. It can also be activated from the Windows menu of MDaemon's menu bar.

### 4.1.16.3 Windows Event Log



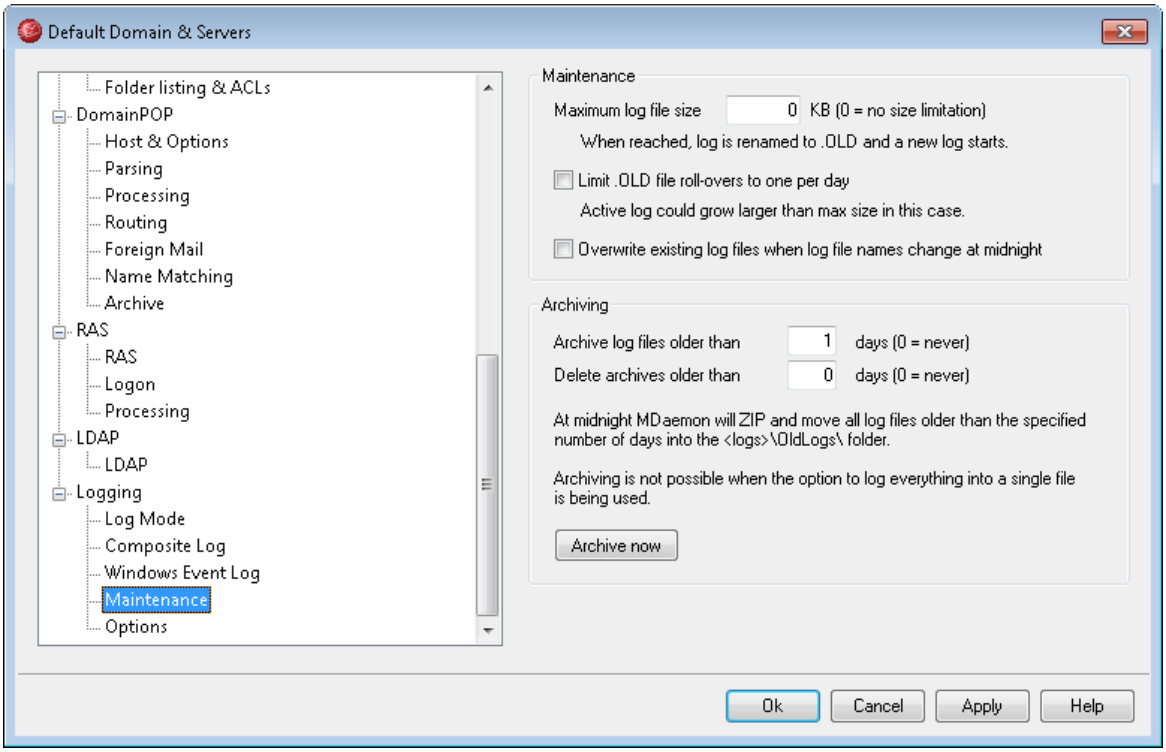

**Use Windows Event Log**
Click this check box if you want to log critical system errors, warnings, and certain other events into the Application section of the Windows Event Log.

**Log the following events:**
If you are logging Windows Events, use this set of options to specify which events

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

you wish to log.

### 4.1.16.4 Maintenance




#### Maintenance

**Maximum log file size [xx] KB**
This is the maximum size in kilobytes that a log file may reach. Once this size is reached, the log file is `copied` to `LOGFILENAME.OLD` and a new log is started.

**Limit .OLD file roll-overs to one per day**
When limiting the log file size, click this checkbox if you want no more than one log file to be backed up per day. Each day, the first time that the maximum log file size is reached it will be renamed to "`*.OLD`" and saved normally. The subsequent log file will continue to grow regardless of the maximum size specified. It will not be rolled over until the next day — even if the maximum size setting is surpassed.

**Overwrite existing log files when log file names change at midnight**
By default, when MDaemon changes the log file's name at midnight and the filename to which it is changing already exists, it will append newly logged information to the existing file. For example, if MDaemon is changing from Monday.log to Tuesday.log and a file named Tuesday.log already exists, it will append newly logged data to the existing file rather than overwrite it or create a new one. Click this checkbox if you want MDaemon to overwrite any existing file rather than append new data to it.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

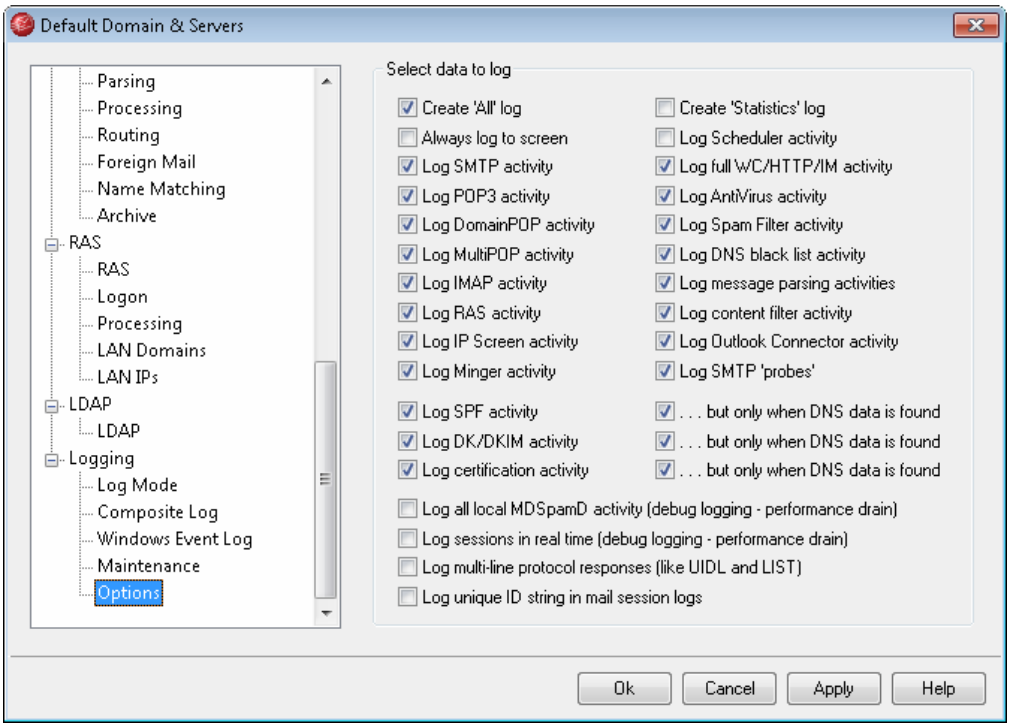
### Archiving

**Archive log files older than [XX] days (0=never)**
Click this option if you want MDaemon to archive each log file whose age exceeds the number of days specified. Each day at midnight, MDaemon will `ZIP` old `*.log` and `*.old` files and move them to the `\Logs\OldLogs\` subfolder (deleting the original files in the process). This process will not archive or delete files that are in use, nor will it archive files when the "*Create a standard set of log files*" option is selected on the Log Mode 99 screen.

**Delete archives older than [XX] days (0=never)**
Use this option if you want MDaemon to delete archived log files automatically when their age exceeds the number of days specified here. Use "0" in this option if you do not wish to delete archives automatically. Archive deletion occurs during the daily midnight cleanup event.

**Archive now**
Click this button to archive old log files immediately rather than waiting for MDaemon to archive them automatically at midnight.

## 4.1.16.5 Options




### Log Options

**Create 'All' log**
Click this option if you want the "`*-all.log`" file to be generated, which contains

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

a composite of all logged activities.

**Always log to screen**
Click this option if you want the logged data to be copied to the MDaemon GUI even when it is minimized or running in the tray.

When this control is cleared, log data isn't copied to the Event Tracking pane when MDaemon is running in the system tray. Consequently, the most recent activity won't be listed on any of the Event Tracking pane's tabs when MDaemon is first opened. It will begin displaying newly logged information from that point forward.

**Log SMTP activity**
Enable this option if you want to log all of MDaemon's send/receive SMTP activity.

**Log POP3 activity**
Click this checkbox to log all POP mail activity. This will log your users' POP mail collection sessions.

**Log DomainPOP activity**
Click this checkbox to log all DomainPOP mail activity.

**Log MultiPOP activity**
Click this checkbox to log all of your users' MultiPOP mail collection activity.

**Log IMAP activity**
Enabling this option causes all of your users' IMAP sessions to be included in MDaemon's log files.

**Log RAS activity**
Click this switch if you want MDaemon to copy RAS dialup/dialdown activities into the log file. This information is useful for diagnosing dialup problems.

**Log IP Screen activity**
Click this checkbox if you want the IP Screening activities to be included in MDaemon's log file.

**Log Minger activity**
Click this checkbox to log Minger server activities.

**Create 'Statistics' log**
Because the statistics log file can potentially use a lot of disk space and CPU power to maintain, this option makes it possible for you to control whether or not that file will be created. The switch is disabled by default.

**Log Scheduler activity**
Enable this checkbox if you wish to log all of the Event Scheduler's 145 activity.

**Log full WC/HTTP/IM activity**
Click this option if you wish to log all WorldClient, HTTP, and ComAgent instant messaging activity. When disabled, WorldClient and HTTP logs will still be created

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

showing WorldClient's startup and shutdown times, but other WC/HTTP/IM activity will not be logged.

**Log AntiVirus activity**
This option logs SecurityPlus for MDaemon activities

**Log Spam Filter activity**
Logs all Spam Filter activity.

**Log DNS black list activity**
This option causes MDaemon to log DNS black list activity. Using this option will allow you to have an easy reference to the sites that were logged as blacklisted.

**Log message parsing activities**
MDaemon periodically performs a great deal of message parsing activity when determining to whom a message should be delivered. Enable this switch if you want this information to be included in the log file.

**Log content filter activity**
Click this checkbox if you want to include Content Filter activity in the log file.

**Log Outlook Connector activity**
This option governs whether or not Outlook Connector activities are logged.

**Log SMTP 'probes'**
Click this option to log SMTP sessions when no message data is transmitted by the sending server (i.e. the sending server does not use the DATA command).

**Log SPF activity**
Click this check box if you wish to log all Sender Policy Framework lookup activities.

> **...but only when DNS data is found**
> If you are logging SPF activities, click this check box if you wish to log only lookups where actual SPF data is found during the DNS lookup, rather than logging all SPF lookups.

**Log DK/DKIM activity**
Click this option if you wish to log DomainKeys (DK) and DomainKeys Identified Mail (DKIM) activity.

> **...but only when DNS data is found**
> Click this check box if you are logging DomainKeys activity but wish to log only those instances where DNS data is found instead of logging all activity.

**Log certification activity**
Use this option if you wish to log message certification.

> **...but only when DNS data is found**
> If you are logging message certification activity, click this check box if you wish to log it only when actual certification data is found during the DNS lookup.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Log all local MDSpamD activity (debug logging—performance drain)**
Use this option to log all local MDSpamD activities (see Caution below).

**Log sessions in real time (debug logging—performance drain)**
Ordinarily, session information is logged after the session is completed in order to conserve resources. Click this option if you want session information to be logged as it occurs.

When using either or both of the previous two logging options, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use these options for debugging purposes.

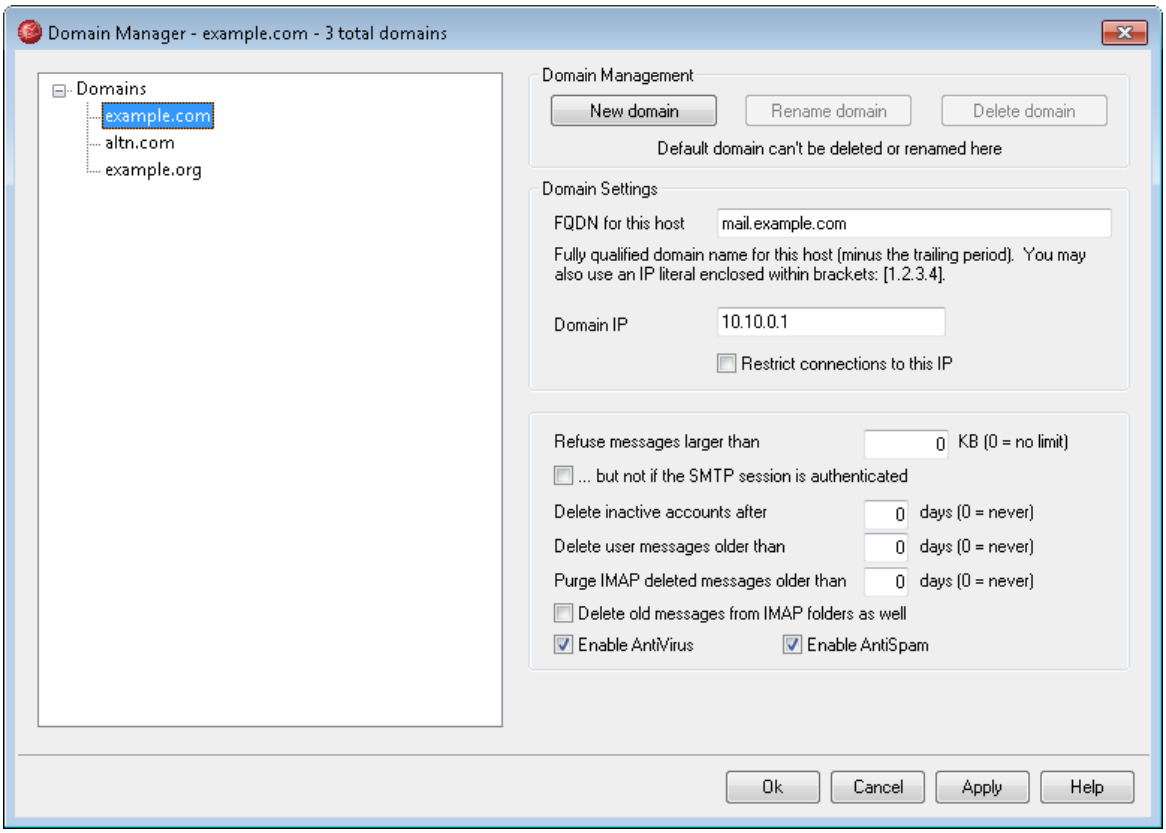
**Log multi-line protocol responses (like UIDL and LIST)**
Sometimes the responses to protocol requests require more than one line of information. Click this checkbox if you want to log these additional lines.

Enabling this switch could potentially increase the amount of logged information a great deal. Because the number of lines in a response can't be determined in advance, and because some responses have great potential for "filling up" your log file with possibly unnecessary information (POP TOP, for example, lists the actual contents of the message), we do not recommend using this feature if log file size or verbosity is of concern to you.

**Log unique ID string in mail session logs**
Click this check box if you wish to include `[%d:%d]` unique ID strings in session logs.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## 4.2 Domain Manager




MDaemon PRO contains full support for multiple domains, administered using the Domain Manager. Here you can manager the domain names, IP addresses, account and message pruning settings, and other domain-specific options for the Default Domain 40 and your other domains. There are a number of additional options specific to the Default Domain that can only be configured from the Default Domain & Servers 40 dialog.

MDaemon supports both single and multiple IP addresses, and IP addresses can be unique to individual domains or shared between them. Further, several key features such as Accounts, Mailing Lists, and some Security Settings are on a per domain basis. When you create an account, for example, you must specify the domain to which the new account belongs. The same goes for Mailing Lists. This also means that features such as the IP Screen 302 and IP Shield 273 are tied to domains individually. Some features, however, such as Name Matching 90 under DomainPOP 81, are tied exclusively to the Default Domain.

To support MDaemon's handling of system messages, the following default Aliases 398 point several reserved mailbox names to MDaemon's default domain name rather than to its other domains:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Finally, in order to support multiple domains, by default MDaemon requires users to use their full email address (e.g. "user01@example.com") as their login value rather than using just the mailbox portion of the address (i.e. "user01"). Some very old mail clients, however, do not support using '@' in the login field. Therefore to accommodate those clients you can specify an alternate character on the System 195 screen under Preferences. Further, this value can be up to 10 characters long, making it possible to provide a string of characters to serve as the delimiter instead of only a single character such as '$'. For example, using '.at.' will allow you to make logon values of "user02.at.example.com". You can also disable the full email address requirement, allowing the use of only the mailbox portion of the address as the login value, but that is not recommended and can cause problems when you have more than one domain.

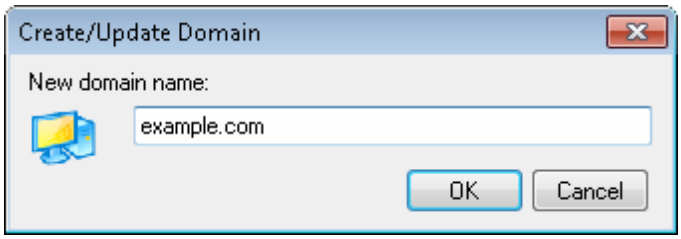
### Domains

The area on the left side of this dialog contains the list of your Domains. The Default Domain 41 is listed first and all other domains are listed alphabetically. Click any domain in the list to view or edit its settings. To create a new domain, click *New domain* on the right.

### Domain Management

#### New domain

To create a new domain: click *New domain*, enter the domain name in the Create/Update Domain dialog, and click *OK*.




#### Rename domain

To change a domain name: select a domain, click *Rename domain*, type the new domain name in the Create/Update Domain dialog, and click *OK*.

#### Delete domain

To delete a domain: select the domain, click *Delete domain*, and confirm your decision to delete the domain by clicking *Yes*.

You cannot delete the default domain, and you cannot rename it from the Domain Manager. Use the options at Default Domain/Servers » Domain 41 to rename the Default Domain.

### Domain Settings

#### FQDN for this host

This value is the Fully Qualified Domain Name (FQDN) that will be used in the SMTP HELO/EHLO instruction when sending mail for this domain. For incoming connections,

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

if the *Restrict connections to this IP* option below is used, the domain is bound to its own IP address and the proper FQDN will be used for connections made to that domain. Using the "*Restrict...*" option, however, is not strictly required for this to work. But, if you have two or more domains using the same unbound IP address then the FQDN used will be the one that is associated with the domain that is first in alphabetical order.

In most cases the FQDN will be either the *Domain name* above or a subdomain of it (for example, "`mail.example.com`"), but an IP literal syntax such as "`[192.0.2.0]`" may also be used. When no FQDN value is specified, MDaemon will use the Default Domain's FQDN.

**Domain IP**
Enter the IP address to associate with the domain being added or edited.

**Restrict connections to this IP**
Click this checkbox if you want to restrict connections to the domain to its *Domain IP* address. By default this only applies to inbound connections. Outbound socket binding is governed by an option under "Preferences » System 195."

---

**Refuse messages larger than XX KB (0=no limit)**
Use this option if you wish to refuse messages for this domain that are larger than the size designated. Use "0" in this option if you do not wish to limit message size.

**...but not if the SMTP session is authenticated**
Check this box if you do not wish to refuse larger messages when the SMTP session is authenticated. Authenticated sessions will be exempt from `SIZE` checks.

## Inactive Accounts and Old Messages

The following four options have corresponding options on the Accounts Editor 366, which can be used to override these default settings for individual accounts.

**Delete inactive accounts after [XX] days (0=never)**
Specify the number of days that you wish to allow an account belonging to this domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

**Delete user messages older than [XX] days (0=never)**
A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

**Purge IMAP deleted messages older than [XX] days (0 = never)**
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this domain's users' folders. Messages flagged for deletion longer than this number of days will be purged from their

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

**Delete old messages from IMAP folders as well**
Click this checkbox if you want the "*Delete messages kept by users...*" option above to apply to messages in IMAP folders as well. When this option is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

---

**Enable AntiVirus**
If *SecurityPlus for MDaemon* 210 is installed, click this check box if you want the SecurityPlus settings to be applied to the selected domain.

**Enable AntiSpam**
Click this check box is you want MDaemon's current Spam Filter settings to be applied to the selected domain.

---

**See:**

**Default Domain & Servers** 40
**Preferences » System** 195

# 4.3 Web & IM Services

## 4.3.1 WorldClient (web mail)

### 4.3.1.1 Overview

WorldClient is a web-based email solution included in MDaemon and designed to offer users email client functionality using their favorite web browser. WorldClient can easily hold its own against traditional mail clients while providing the added bonus of its ability to enable users to access their email from anywhere at anytime as long as they have an Internet or network connection. Further, because all of their email folders, contacts, calendars, and so on reside on the server instead of on their local computer, they can have access to everything as if they were at their desk.

WorldClient provides many benefits to email administrators. Since WorldClient isn't workstation dependent you can configure everything from the server, unlike many client applications. This saves you from having to configure and maintain each individual email client. You can also customize the graphical images and HTML pages used in WorldClient to suit your corporate needs, or the needs of your customer. Further, you can give your users the ability to maintain their own account settings thus saving you time — you can give as much or as little control to your users as you want.

Finally, in addition to the convenience of having a web-based client, there are many additional features that will benefit your users, such as: extensive email functionality, client-side interface available in almost 30 languages, personal and global address

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

books, manageable mail folders and filters, send/receive file attachments, multiple visual "themes" for the interface, themes for mobile devices, calendar features, groupware features, an integrated instant messenger that can be downloaded to your desktop, and much more.

## Calendar & Scheduling System

MDaemon is equipped with a complete collaboration system. From within WorldClient you can easily create appointments, schedule meetings, and work with address books. Recurring appointments are fully supported, and appointments have many fields available to describe them. Further, contacts, calendars, and task data are stored as IMAP folders within each user's root mail directory. Through WorldClient, your users can access these personal folders and control which other users have access to them. All WorldClient themes (especially Lookout) have templates that present contact, calendar, notes, and task folders in a logical and attractive way.

Because the Calendar system is integrated with MDaemon, there is the added benefit of email notifications of appointments, whether scheduled by you or a third-party. Whenever someone other than yourself schedules an appointment for you, you will receive an email message summarizing the appointment. Each designated appointment attendee will receive an email message detailing the appointment's date, time, location, subject, and list of attendees. Further, any attendees who have calendar entries that conflict with the appointment's time slot will receive a message notifying them of the appointment and its conflict with their schedule. The person who scheduled the meeting will receive a summary message listing all of the meeting's details and invited attendees who did or did not have scheduling conflicts.

The Calendar System is also equipped with support for Internet Calendar (iCal) used by Microsoft Outlook and other iCalendar compliant email programs. The Calendar System can detect and process iCalendar information sent to your users and update their calendars accordingly. When a user opens an iCalendar attachment from within WorldClient the information contained in the attachment will be reflected in the user's WorldClient calendar. Also, when users create new meetings or appointments they can list one or more email addresses to which they wish an iCalendar email to be sent. This feature can be set by individual users in their WorldClient options.

## ComAgent

ComAgent is MDaemon's secure instant messaging system, address book client, and tray applet that provides quick access to WorldClient's email features. ComAgent can be downloaded by each WorldClient user and then installed on the individual's local computer. It is pre-configured for the specific user when downloaded thus limiting the need to configure it manually.

ComAgent runs in the background and checks your account for new mail by querying the WorldClient server directly. This eliminates the need to open a browser or keep one open to check your email — ComAgent checks for new mail and notifies you with a sound or visual alert when new mail arrives. ComAgent also displays a list of your mail folders and the number and type of messages that each one contains (new, unread, and read). Furthermore, it can be used to launch your browser and move it immediately to a specific mail folder, the first unread message, the compose page, or your calendar page.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Additionally, ComAgent can be used to provide two-way address book synchronization between MDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

Finally, ComAgent is also equipped with a complete instant messaging system. You can view your list of ComAgent "buddies" and each one's online status (online, away, offline), start a conversation with any one or group of them, set your own online status, and view past conversations in a history folder.

For specific instructions on how to use ComAgent, see its online help system.

## ComAgent's Instant Messaging System

ComAgent is equipped with a simple but effective instant messaging (IM) system. With this system you can communicate instantly with any other account on your MDaemon server. You can choose a list of "buddies" from a list of all MDaemon users and then see which ones are online and ready to receive an IM. You will also be able to start a group conversation involving several buddies at once. All of the IM features are available via the tray icon's shortcut menu, and from the ComAgent window.

ComAgent's IM system is also scriptable, which allows custom programs to interface with it. By creating semaphore (`SEM`) files in the \MDaemon\WorldClient\ folder, an external application can send instant messages to your ComAgent users. The following is the format of the SEM file:

| | |
|---|---|
| `To: user1@example.com` | Email address of ComAgent user. |
| `From: user2@example.com` | Email address of instant message's sender. |
| `<blank line>` | |
| `Text of instant message.` | This is the text sent as an instant message. |

The `SEM` file name must start with the characters "`IM-`" and be followed by a unique numerical value. For example, "`IM-0001.SEM`". Applications should also create a corresponding file called "`IM-0001.LCK`" to lock the `SEM` file. Once the `SEM` file is completed remove the `LCK` file and the `SEM` file will be processed. MDaemon uses this scripting method to send Instant Message reminders to you about upcoming appointments and meetings.

The Content Filter system is equipped with an Action that uses this scripting method to send instant messages. Further, rules utilizing this action can use the Content Filter macros in the IM. For example, you could create a rule to send an instant message rule containing lines like this:

```
You have received an email from $SENDER$.
Subject: $SUBJECT$
```

This rule would be an effective way to send new mail alerts through ComAgent.

Because many businesses and administrators have reservations about using an Instant Messaging system in their company due to the inherent lack of centralized accountability and the inability to monitor IM traffic that is in traditional and well known IM clients, we have designed ComAgent's instant messaging system to minimize

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

those deficiencies. First of all, our system is not peer-to-peer — individual ComAgent clients do not connect directly to each other. Further, because every IM passes through the server, each message is logged in a central location accessible to the MDaemon/WorldClient administrator. Thus a record of all conversations can be maintained for the security of both your company and your employees or users. IM activity is logged in a file called `InstantMessaging.log` located in the `MDaemon\LOGS\` directory. The assurance of accountability is also the primary reason we do not support other IM clients such as ICQ, AOL, and MSN. Finally, ComAgent's IM system is secure in that each transaction is strongly encrypted from start to finish so that plain text is never transmitted.

Instant Messaging is provided on a per-domain basis. Controls for activating instant messaging and designating whether or not IM traffic should be logged are located on the ComAgent/IM screen of the WorldClient dialog (`Setup » Web & IM Services » ComAgent/IM`).

### ComAgent Skins

ComAgent's interface is compatible with *msstyles* skins, which are readily available on the internet. Several styles are included, but to install a new style, download the `*.msstyles` file and place it under ComAgent's `\Styles\` folder in a subfolder with the same name as the file. For example, if the file was called `Red.msstyles` then the path for the file would be: "`\.\Styles\Red\Red.msstyles`"

## Automatic Address Book Synchronization

By using ComAgent in conjunction with MDaemon's integrated address book system, you can provide two-way synchronization between MDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

MDaemon maintains an accurate and continuously up to date database of users each time an MDaemon account is added, removed, or modified. ComAgent has the ability to query MDaemon at regular intervals and acquire all the contact information being stored there. It then publishes this information to the local computer's Windows Address Book or contact store. This has the effect of instantaneously updating any local software package which uses the local address book system (for example, Outlook/Outlook Express).

Anyone using ComAgent with the proper access credentials can also add Public contacts by using the Windows Address Book directly, or through Outlook/Outlook Express. The new contact will be picked up by ComAgent and uploaded to MDaemon's address book. From there all other users on your network will have access to the new contact the next time their ComAgent queries MDaemon.

On the Synchronization screen of ComAgent's Preferences dialog you can specify the folders within your Windows Address Book that you wish to be synchronized. You can designate separate folders for both Public and Private contacts.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Windows Address Book (WAB) synchronization requires IE 5 or greater with identity support enabled.

**For more Address Book options, see:**

**WorldClient (web mail) » ComAgent/IM** 124
**LDAP** 97
**Windows Address Book** 418

### 4.3.1.2 Using WorldClient

## Starting WorldClient

There are three ways to start/stop the WorldClient server:

1. In the Stats pane on the left-hand side of the MDaemon GUI, right-click on the WorldClient entry and choose the *Toggle Active/Inactive* selection on the shortcut menu.
2. Click "File » Enable WorldClient" server on the main interface.
3. Click "Setup » Web & IM Services" on the main interface, and then click *WorldClient runs using built-in web server* on the Web Server screen.

## Logging in to WorldClient

1. Point your web-browser to `http://example.com:WCPortNumber`. This port is designated on the Web Server 116 screen of the WorldClient section. If you configure WorldClient to listen to the default web port (port 80) then you do not need to denote the port number in the login URL (e.g. `www.example.com` instead of `www.example.com:3000`).
2. Type your MDaemon account's user name and password.
3. Click Sign-in.

## Changing WorldClient's Port Setting

1. Click "Setup » Web & IM Services" on the menu bar.
2. Type the desired port number in the control labeled *Run WorldClient Server using this TCP Port.*
3. Click OK.

## Client-side Help

WorldClient is equipped with extensive client-side help for your users. See the online help system within WorldClient for information on the client features and functions.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

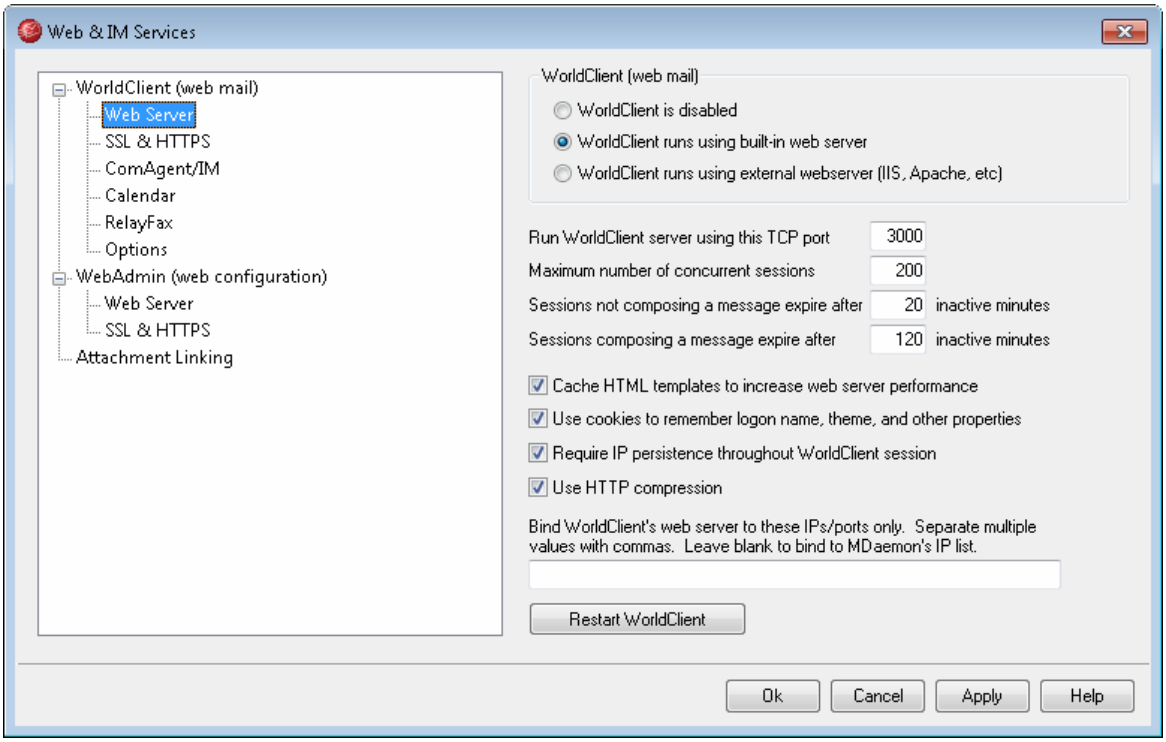
### 4.3.1.3 WorldClient (web mail)

Use the "Setup » Web & IM Services » WorldClient (web mail)" menu selection to enable your WorldClient server and configure various WorldClient related settings. You can designate the port on which it will operate as well as the time that you wish to allow WorldClient sessions to remain inactive before they expire. You can also control many global or domain specific settings such as: the default language and theme to use, whether users can create accounts, the default pagination of the message listing, whether or not ComAgent support is enabled, whether or not Instant Messaging is allowed and logged, configure support for SSL and Certificates, RelayFax integration, and much more.

Click the links below for information on the various WorldClient sections.

**Web Server** 116
**SSL & HTTPS** 121
**ComAgent/IM** 124
**Calendar** 125
**RelayFax** 127
**Options** 129

#### 4.3.1.3.1 Web Server




This screen contains various global, server level settings that govern WorldClient's configuration and behavior regardless of the users or domains to which they belong.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## WorldClient Properties

**WorldClient is disabled**
Choose this option to disable WorldClient. You can also toggle WorldClient active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

WorldClient must be active when using the Attachment Linking 142 feature.

**WorldClient runs using built-in web server**
Choose this option to run WorldClient using MDaemon's built-in web server. You can also toggle WorldClient active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

**WorldClient runs using external web server (IIS, Apache, etc)**
Choose this option when you wish to run WorldClient under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see Running WorldClient under IIS 118

**Run WorldClient server using this TCP port**
This is the port on which WorldClient will listen for connections from your users' web browsers.

**Maximum number of concurrent sessions**
This is the maximum number of sessions that may be connected to WorldClient at the same time.

**Sessions not composing a message expire after xx inactive minutes**
When a user is logged in to WorldClient but is not composing a message, this is the amount of time that their session will remain inactive before WorldClient will close it.

**Sessions composing a message expire after xx inactive minutes**
This timer governs how long a user's session will be kept open while they are composing a message and the session remains inactive. It is a good idea to set this timer higher than the *Sessions not composing a message...* timer, since inactivity time is typically greater while a user is composing a message. This is because composing a message requires no communication with the server until the message is sent.

**Cache HTML templates to increase web server performance**
Click this box to cause WorldClient to cache templates in memory rather than read them each time they need to be accessed. This can dramatically increase server performance but WorldClient will have to be restarted if you ever make a change to one of the template files.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Use cookies to remember logon name, theme, and other properties**
Click this option if you want WorldClient to store each user's logon name, theme, and certain other properties in a cookie on his or her local computer. Using this feature gives your users a more "customized" login experience but requires that they have support for cookies enabled in their browsers.

**Require IP persistence throughout WorldClient session**
As an added security measure you can click this checkbox to cause WorldClient to restrict each user session to the IP address from which the user connected when the session began. Thus, no one can "steal" the user's session since IP persistence is required. This configuration is more secure but could cause problems for users who may be using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

**Use HTTP Compression**
Click this check box if you want to use HTTP compression in your WorldClient sessions.

**Bind WorldClient's web server to these IPs/ports only**
If you wish to restrict the WorldClient server to only certain IP addresses or ports then specify those IPs and ports here separated by commas. Use the format: "`IP_address:Port`" to designate a port (for example, `192.0.2.0:80`). If you do not include a port, then the default TCP port specified above and the default HTTPS port specified on the SSL & HTTPS 121 screen will be used. Use "`*`" if you want WorldClient to listen on all ports. For example, "`*,*:80`" would cause WorldClient to listen on all IP addresses, on the default ports specified (3000 and 443), and it would also listen on all IP addresses on port 80. If you leave this field blank then WorldClient will monitor all IP addresses designated for your Domains 108.

**Restart WorldClient (required when port or IIS value changes)**
Click this button if you wish to restart the WorldClient server. Note: when changing WorldClient's port setting you must restart WorldClient in order for the new setting to be recognized.

### 4.3.1.3.1.1 Running WorldClient under IIS6

WorldClient is equipped with a built-in web server and therefore doesn't require Internet Information Server (IIS) to operate. However, WorldClient does support IIS, and can therefore function as a ISAPI DLL. The following information on how to configure WorldClient to operate under IIS6 was taken from article #01465 of the MDaemon Knowledge Base at www.altn.com:

1. Open the Internet Information Services Management Console.
2. Right-Click on **Application Pools**.
3. Choose **New/Application Pool**.
4. Name the Pool **Alt-N** and click the **OK** button.
5. Right-Click on **Alt-N**.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

6. Click on **Properties**.
7. Click on the **Performance** tab.
8. Uncheck the options for **Shutdown worker processes after being idle for (time in minutes)**: and **Limit the kernel request queue (number of requests)**.
9. Click on the **Identity** tab.
10. In the drop-down for Predefined, choose **Local Service**.
11. Click the **OK** button.
12. Right-Click on **Web Sites**.
13. Choose **New**.
14. Click on **Web Site**. (This will launch a wizard)
15. Click on the **Next** button.
16. Type in a name for the site such as **WorldClient**.
17. Click on the **Next** button.
18. Click on the **Next** button again.
19. Browse to the Home directory: which will be **C:\MDaemon\WorldClient\HTML** with a default installation.
20. Click on the **Next** button.
21. Make sure the options for **Read**, **Run Scripts**, and **Execute** are checked.
22. Click on the **Next** button.
23. Click on the **Finish** button.
24. Right click on the website you just made **(WorldClient)**.
25. Choose **Properties**.
26. Click on the **Documents** tab.
27. Remove all listed documents.
28. Add **WorldClient.dll**.
29. Choose the **Home Directory** tab.
30. Choose **Alt-N** in the Application Pool drop-down.
31. Click the **OK** button.
32. Click on **Web Service Extensions**.
33. Enable **All Unknown ISAPI Extension** or Create a new one for **WorldClient.DLL**.

The Internet Guest Account - **IUSER_<SERVER_NAME>** - needs **Full Access** NTFS permissions for the MDaemon directory and all sub-directories.

1. Right-Click on the MDaemon directory. (C:\MDaemon)
2. Select **Properties**.
3. Select the **Security** tab.
4. Click the **Add** button.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

5. Click the **Advanced** button.
6. Click the **Find Now** button.
7. Select **IUSER_<SERVER_NAME>** (where "<SERVER_NAME>" is the name of the local computer).
8. Click the **OK** button.
9. Click the **OK** button.
10. Check the box for **Full Control**.
11. Click the **OK** button.

These same steps need to be applied to any directory MDaemon is configured to use.

When doing upgrades to MDaemon after setting up the web:

1. Open the Internet Information Services Management Console.
2. Open **Application Pool** list.
3. Right-Click **Alt-N**.
4. Choose **Stop**.
5. Shutdown MDaemon.
6. Install the upgrade.
7. Once installation is complete, start MDaemon.
8. In Information Services Management Console again, Right-Click **Alt-N**.
9. Choose **Start**.

If you follow the above method, the following should occur.

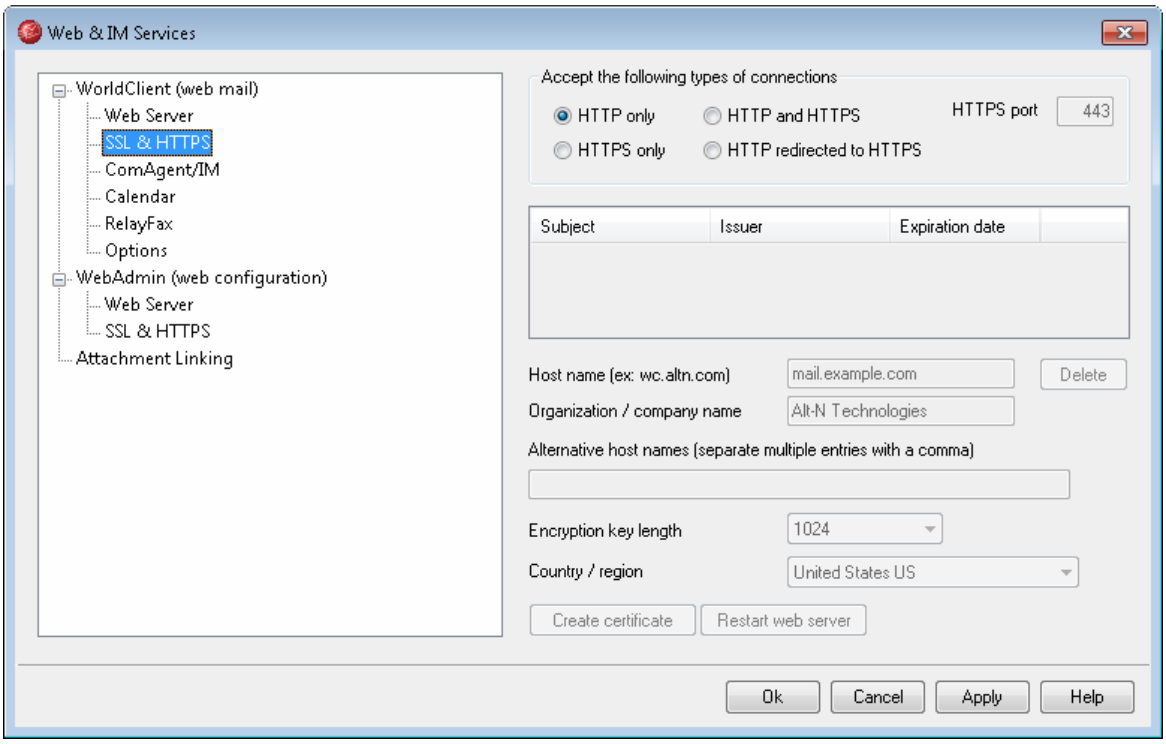
1. After stopping the **Application Pool** users will get a message **Service Unavailable**.
2. Following these steps should help minimize your chances of having to reboot your computer after upgrading MDaemon.

The setup of this program under IIS is NOT supported by tech support and those who choose to run WC under IIS must be aware of all security issues and ramifications of running any applications under IIS. It is recommended that all Patches and updates be installed on IIS before the installation of WorldClient as an ISAPI extension.

When running WorldClient under IIS you will no longer be able to start and stop it from MDaemon's interface. You must use the tools provided with IIS to do so.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.3.1.3.2 SSL & HTTPS




MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WorldClient to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » WorldClient (web mail)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WorldClient".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 309

This screen only applies to WorldClient when using MDaemon's built-in web server. If you configure WorldClient to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Accept the following types of connections

**HTTP only**
Choose this option if you do not wish to allow any HTTPS connections to WorldClient. Only HTTP connections will be accepted.

**HTTP and HTTPS**
Choose this option if you want to enable SSL support within WorldClient, but do not wish to force your WorldClient users to use HTTPS. WorldClient will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the WorldClient TCP port designated on the Web Server 116 screen of WorldClient (web mail).

**HTTPS only**
Choose this option if you wish to require HTTPS when connecting to WorldClient. WorldClient will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

**HTTP redirects to HTTPS**
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

**HTTPS port**
This is the TCP port that WorldClient will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WorldClient's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WorldClient port that is designated on the Web Server 116 screen of WorldClient (web mail). If you are still allowing HTTP connections to WorldClient then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

### Certificates

This box displays your SSL certificates. Single-click a certificate in this list to designate it as the certificate that you wish WorldClient to use. Double-click a certificate to open it in the Certificate dialog to review its details or edit it.

MDaemon does not support multiple certificates for WorldClient. All WorldClient domains must share a single certificate. If you have more than one WorldClient domain then enter those domain names (and any others that you wish to use to access WorldClient) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Delete**
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

**Host name**
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

**Organization/company name**
Enter the organization or company that "owns" the certificate here.

**Alternative host names (separate multiple entries with a comma)**
MDaemon does not support multiple certificates — all WorldClient domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

**Encryption key length**
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

**Country/region**
Choose the country or region in which your server resides.

**Create Certificate**
After entering the information into the above controls, click this button to create your certificate.

**Restart web server**
Click this button to restart the web server. The web server must be started before new certificates will be used.

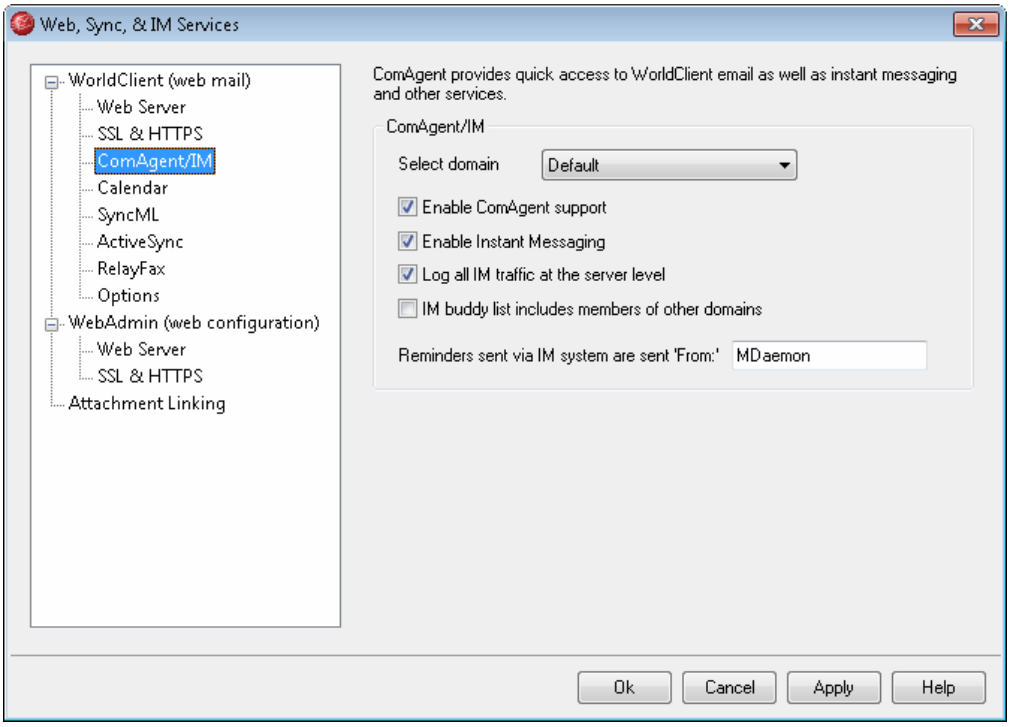
---

**See:**

**SSL & Certificates** 309
**Creating and Using SSL Certificates** 320

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.3.1.3.3 ComAgent/IM




This dialog controls various aspects of the ComAgent tray applet and instant messenger. You can set these options specifically for each domain.

#### ComAgent/IM

**Select domain**
Use this drop-down list to choose the domain whose settings you wish to edit. Leave it set to *Default* if you wish to edit the default settings. The default settings will be used for all domains whose settings you haven't specifically changed. If you make changes to any of the settings and then select a different domain from the list, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

**Enable ComAgent support**
This option makes the ComAgent messaging utility available to the selected domain's users. They can download it from the Options » ComAgent page within WorldClient. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier.

**Enable Instant Messaging**
Click this option if you want to activate ComAgent's instant messaging (IM) system for the selected domain's users. Clear the check box if you want the instant messaging controls to be unavailable.

**Log all IM traffic at the server level**
Click this check box if you want all of the selected domain's instant messaging

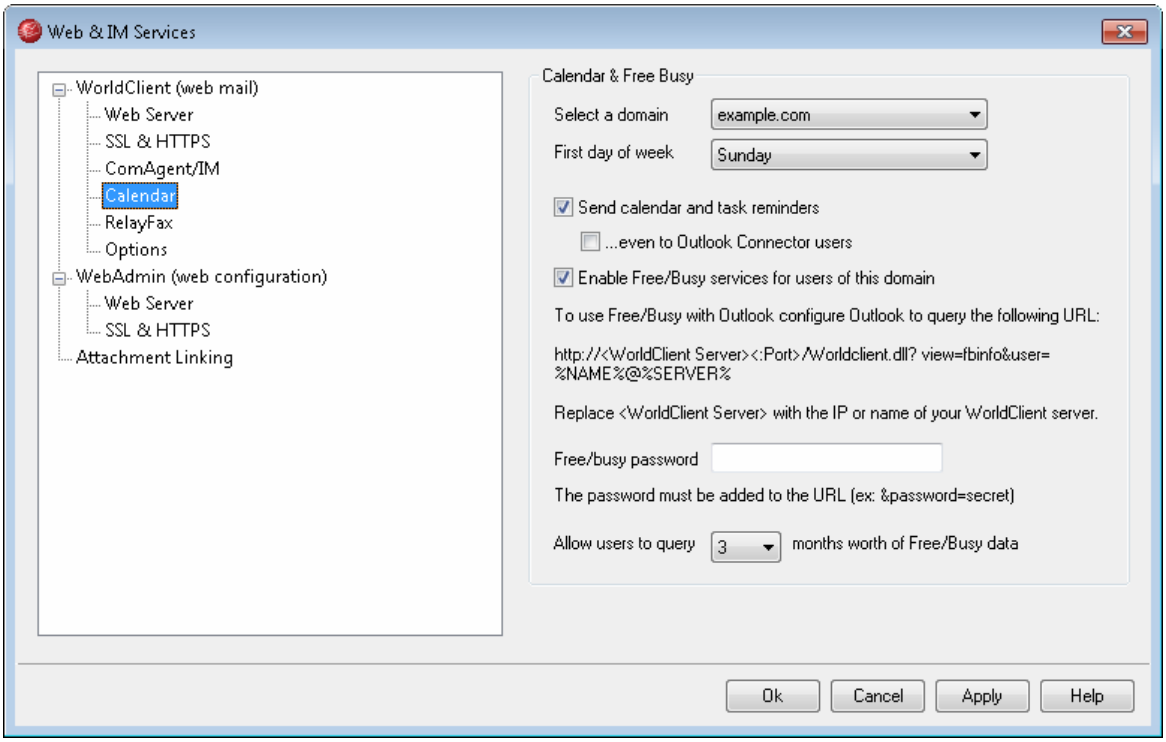
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

traffic to be included in the `InstantMessaging.log` file (located in the `MDaemon/LOGS/` folder).

**IM buddy list includes members of other domains**
Click this option if you want all of your MDaemon users (regardless of the domain) to be available for adding to the selected domain's buddy lists. Clear this checkbox if you want only users of the same domain to be available for adding to buddy lists. For example, if your MDaemon is hosting mail for example.com and example.org, then activating this control for your example.com users will enable them to add buddies to their lists from both domains. Clearing it would mean that they could only add other example.com users.

**Reminders sent via IM system are sent 'From:' [ *text* ]**
When an Appointment is scheduled on a user's WorldClient calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message if he or she is using ComAgent. Use this text box to specify the name that you wish the message to appear to be 'From:'.

### 4.3.1.3.4 Calendar




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Calendar & Free Busy

**Select a domain**
Use this drop-down list to select the domain whose Group Scheduling and Calendar settings you wish to edit. If you make changes to any settings and then attempt to select a different domain from the list, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

**First day of week**
Choose a day from the drop-down list. The selected day will appear in the domain's calendars as the first day of the week.

**Send calendar and task reminders**
Click this checkbox if you wish to allow WorldClient's calendar and task reminders to be sent to your users via email and ComAgent.

**...even to Outlook Connector users**
If you have enabled the "*Send calendar and task reminders*" option above, click this option if you also wish to enable reminders for Outlook Connector users.

## Free/Busy Options

MDaemon includes a Free/Busy server, which makes it possible for a meeting planner to view the availability of potential meeting attendees. To access this feature, click Scheduling within WorldClient when creating a new appointment. This opens a Scheduling window containing the list of attendees and a color-coded calendar grid with a row for each one. Each attendee's row is color-coded to indicate the times at which he or she might be available for a meeting. There are colors for Busy, Tentative, Out of Office, and No information. There is also an Auto-Pick Next button that makes it possible for you to query the server for the next time slot at which all attendees may be available. When you have finished creating the appointment it will send an invitation to all of the attendees, who can then accept or decline.

WorldClient's Free/Busy server is also compatible with Microsoft Outlook. To use it, configure Outlook to query the URL listed below for Free/Busy data. In Outlook 2002, for example, the Free/Busy options are located under "Tools » Options » Calendar Options... » Free/Busy Options..."

Free/Busy server URL for Outlook:

```
http://<WorldClient><:Port>
/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Replace "<WorldClient>" with the IP address or domain name of your WorldClient server, and "<:Port>" with the port number (if you aren't using the default web port). For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

For more on how to use WorldClient's Free/Busy features to schedule your

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

appointments, see the online Help system within WorldClient.

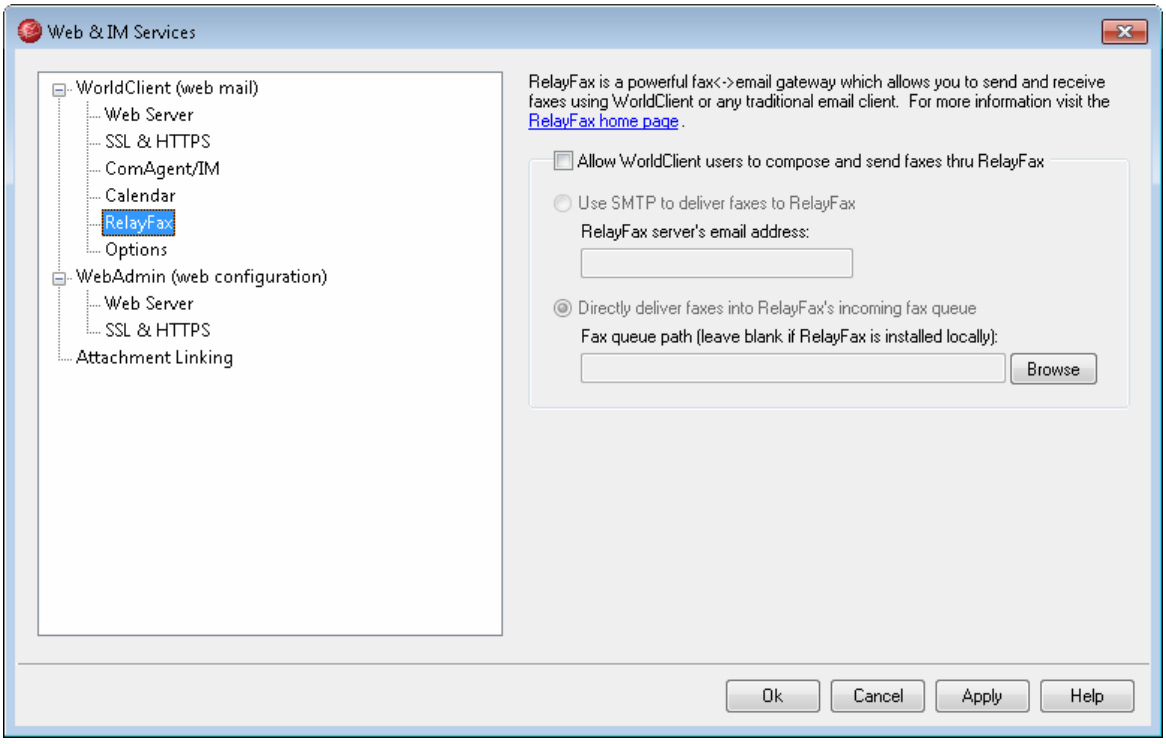
**Enable Free/Busy services for users of this domain**
Click this option if you wish to provide access to the Free/Busy server features to users of the domain selected above.

**Free/Busy password**
If you wish to require a password when this domain's users attempt to access the Free/Busy server features via Outlook, then include the password here. This password must be appended to the URL listed above (in the form: "`&password=FBServerPass`") when the users configure their Free/Busy settings within Outlook. For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER
%&password=MyFBServerPassword
```

**Allow users to query X months worth of Free/Busy data**
Use this option to designate how many months worth of Free/Busy data your users may query.

### 4.3.1.3.5 RelayFax




Alt-N Technologies' RelayFax Server is an email to fax and fax to email gateway that can be seamlessly integrated with WorldClient in order to provide its services to your

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

users. When this functionality is enabled, WorldClient users will be given access to various features that will enable them to compose and send faxes via the WorldClient client pages. For more information, visit the RelayFax section of www.altn.com.

### RelayFax Integration Options

**Allow WorldClient users to compose and send faxes thru RelayFax**
Click this option to integrate RelayFax with WorldClient. When active it will cause a "Compose Fax" control and other fax related features to appear on the WorldClient pages.

**Use SMTP to deliver faxes to RelayFax**
RelayFax monitors a specific mailbox for incoming messages that are to be faxed. Click this option and MDaemon will use the normal SMTP email delivery process to send these messages to that mailbox's address. This option is useful when RelayFax is monitoring a mailbox located somewhere other than your local network. If RelayFax resides on your network you may choose to have MDaemon deliver the messages directly to RelayFax's message queue and thus bypass the SMTP delivery process altogether. For more information on this method, see *Directly deliver faxes into RelayFax's incoming fax queue* below.

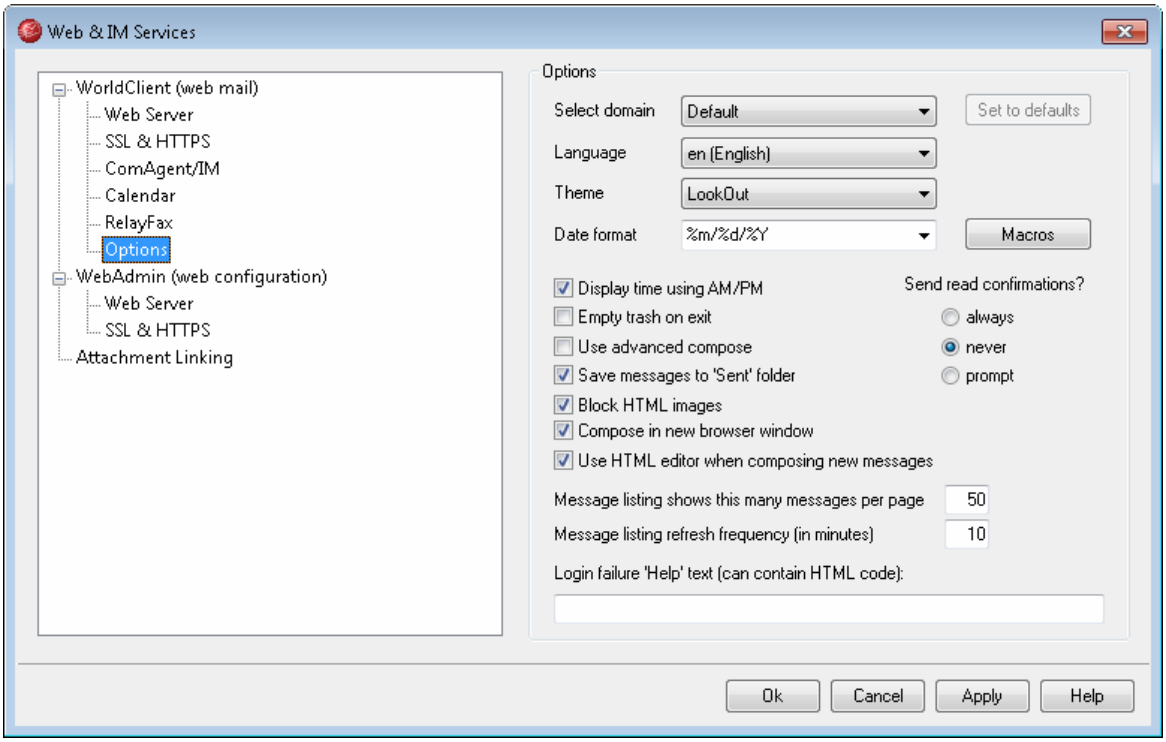
**RelayFax server's email address**
Specify the email address to which you want messages intended for faxing to be delivered. This value must match the address that you have configured RelayFax to monitor for these messages.

**Directly deliver faxes into RelayFax's incoming fax queue**
If RelayFax resides on your LAN you may choose this method rather than SMTP for distributing messages for faxing. When MDaemon receives a message intended for RelayFax it will be placed directly into RelayFax's incoming queue rather than delivered using SMTP.

**Fax queue path**
If RelayFax resides on the same machine on which MDaemon is running, you may leave this file path blank. Otherwise, you must specify the network path to RelayFax's \app\ folder.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.3.1.3.6 Options




The settings on this screen are domain specific and control client-level behavior rather than the overall behavior and configuration of the WorldClient server.

#### Options

**Select domain**
Use this drop-down list to choose the domain whose settings you wish to edit. Leave it set to *Default* if you wish to edit the default settings. The default settings will be used for all domains whose settings you haven't specifically changed. If you make changes to any of the settings and then select a different domain from the list, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

**Set to defaults**
This option resets a domain to the *Default* settings. Use the *Select domain* control to select a domain and then click *Set to defaults* to restore it.

#### Language

Use the drop-down list box to choose the default language in which the WorldClient interface will appear when your users first sign in to the selected domain. Users can change their personal language setting on the WorldClient Sign-in page, and through an option in Options » Personalize within WorldClient.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Theme**

Use this drop-down list box to designate the default WorldClient theme to use for the selected domain's users whenever they sign in for the first time. The users can personalize the theme setting from Options » Personalize within WorldClient.

**Date format**
Use this text box to designate how dates will be formatted for the selected domain. Click the Macros button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

**%A** — Full weekday name

**%B** — Full month name

**%d** — Day of month (displays as "01-31")

**%m** — Month (displays as "01-12")

**%y** — 2-digit year

**%Y** — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in WorldClient as "`12/25/2011`".

This setting is per domain. Individual users cannot modify the date format used for their accounts.

**Macros**
Click this button to display the list of macro codes that can be used in the *Date format*.

**Display time using AM/PM**
Click this option if you want a 12-hour clock with AM/PM to be used within WorldClient for times displayed for this domain. Clear the check box if you want to use a 24-hour clock for the domain. Individual users can modify this setting via the "*Display my hours in an AM/PM format*" option located on the Options » Calendar page within WorldClient.

**Empty trash on exit**
This option causes the user's trash to be emptied when he or she signs out from WorldClient. Individual users can modify this setting from the Options » Personalize page within WorldClient.

**Use advanced compose**
Check this box if you wish the domain's users to see the Advanced Compose screen in WorldClient rather than the normal Compose screen by default. Individual users can modify this setting from Options » Compose within WorldClient.

**Save messages to 'Sent' folder**
Click this option if you want a copy of each message that you send to be saved in

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

your mailbox's *Sent* folder. Individual users can modify this setting from the Options » Compose page within WorldClient.

**Block HTML images**
Enable this check box if you wish to prevent remote images from being displayed automatically when viewing HTML email messages in WorldClient. In order to view the images the user must click the bar that appears above the message in the browser window. This is a spam prevention feature, because many spam messages contain images with special URLs that identify the email address of the user who viewed the images, thus confirming to the spammer that it is a valid, working address. This option is enabled by default.

**Compose in new browser window**
Check this box if you want a separate browser window to open for composing messages instead of simply switching the main window to the compose screen. Clear the box if you do not want separate windows to open. Individual users can modify this setting from the Options » Compose page within WorldClient.

**Use HTML editor when composing new messages**
Check this box if you want the domain's users to see the HTML compose editor by default in WorldClient. They can control this setting for themselves from Options » Compose within WorldClient.

**Send read confirmations?**
This option governs how WorldClient will respond to incoming messages that contain a request for read confirmation.

**always**
If this option is selected, MDaemon will send a notification to the sender indicating that the message was read. The WorldClient user who received the message will not see any indication that the read confirmation was requested or responded to.

**never**
Choose this option if you want WorldClient to ignore read confirmation requests.

**prompt**
Select this option if you wish to ask WorldClient users whether or not to send a read confirmation each time a message is opened that requests it.

**Message listing shows this many msgs per page**
This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from Options » Personalize within WorldClient.

**Message listing refresh frequency (in minutes)**
This is the number of minutes that WorldClient will wait before automatically

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

refreshing the Message Listing. Individual users can modify this setting from Options » Personalize within WorldClient.

**Login page 'Help' text (can contain HTML code)**
You can use this option to specify a sentence of text (either plain text or HTML) to display on the WorldClient sign-in page when a user encounters a problem signing in. The text is displayed below the following default text: "*Incorrect Logon, please try again. If you need assistance please contact your email administrator.*" This text could be used to direct users to a page or contact info for help regarding signing in to WorldClient.

### 4.3.2 WebAdmin (web configuration)

WebAdmin is an application designed to provide support for web-based remote administration of Alt-N Technologies software. WebAdmin is included with MDaemon and supports remote administration of both MDaemon® and its integrated web-based email component, WorldClient®.

WebAdmin is a server application designed to run in the background on the same computer as MDaemon. To access WebAdmin you will simply open your browser and point it to the URL and port number on which WebAdmin resides (e.g. `www.example.com:1000`). After providing your login credentials, you will be given access to various controls and settings within MDaemon. The type and number of settings to which you will have access is dependent upon the level of access given. There are three levels of access that can be provided to WebAdmin users: Global, Domain, and User.

**Global Administrators** — Global administrators are users who have global access permission enabled under their account settings within MDaemon. Global access means that the user can see and configure every setting and control that is accessible via WebAdmin. Global administrators can add, edit, and delete users, domains, and mailing lists. They can edit product INI files, designate other users as Domain administrators, manage passwords, and do many other things; they

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

have complete administrative control.

**Domain Administrators** — Similar to Global administrators, Domain administrators have complete control over all users and product settings accessible via WebAdmin. Their administrative control, however, is limited to the domain or domains to which they have been given access. Domain administrators and the domains over which they have control are designated from within WebAdmin by a Global administrator, or by another Domain administrator with access to those domains.

**Users** — The lowest possible level of WebAdmin access is User access. MDaemon users can sign in to WebAdmin and, for example, view their individual account settings as well as edit their MultiPOP entries, mail filters, Autoresponders, and so on. The type and number of settings that can be edited depends on the permissions given in each user's account settings

Everyone who has permission to access both WorldClient and WebAdmin can access WebAdmin from within WorldClient. WebAdmin is opened in a separate browser window from within WorldClient by clicking the "Advanced Settings" link under "Options".

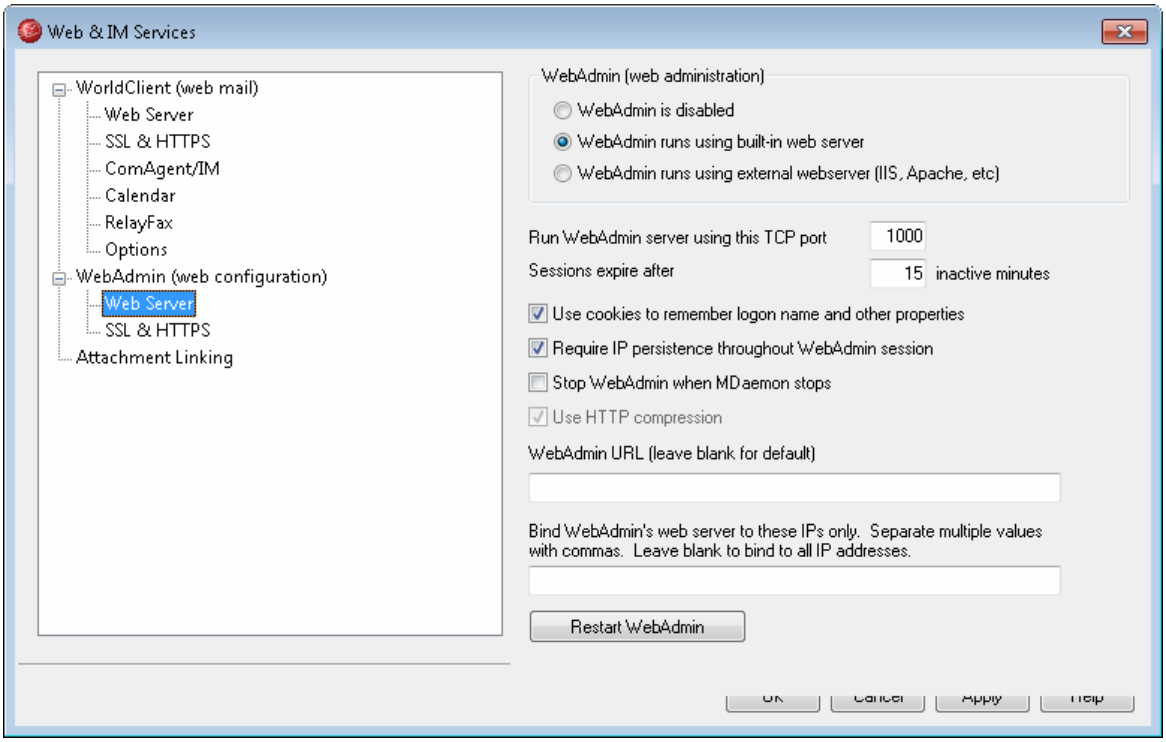
---

**See:**

**WebAdmin » Web Server** 134
**WebAdmin » HTTPS** 136
**New Account Defaults » Web Access Defaults** 387
**Account Editor » Web** 346
**Running WebAdmin under IIS** 138

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.3.2.1 Web Server




#### WebAdmin (web administration)

**WebAdmin is disabled**
Choose this option to disable WebAdmin. You can also toggle WebAdmin active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

**WebAdmin runs using built-in web server**
Choose this option to run WebAdmin using MDaemon's built-in web server. You can also toggle WebAdmin active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

**WebAdmin runs using external web server (IIS, Apache, etc)**
Choose this option when you wish to run WebAdmin under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see Running WebAdmin under IIS 138.

**Run WebAdmin server using this TCP port**
This is the port on which WebAdmin will listen for connections from your web browser. The default port is 1000.

**Sessions expire after xx inactive minutes**
When you are logged in to WebAdmin, this is the amount of time that your session is

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

allowed to be inactive before WebAdmin will close it. The default is 15 minutes.

**Use cookies to remember logon name and other properties**
Click this option if you want WebAdmin to store your logon name and certain other properties in a cookie on your local computer. Using this feature gives you a more customized login experience but requires that they have support for cookies enabled in your browser.

**Require IP persistence throughout WebAdmin session**
As an added security measure you can click this checkbox to cause WebAdmin to restrict each session to the IP address from which you connected when the session began. Thus, no one can "steal" the session since IP persistence is required. This configuration is more secure but could cause problems if you are using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

**Stop WebAdmin when MDaemon stops**
Click this option if you want WebAdmin to be shut down whenever MDaemon is shut down. Otherwise, WebAdmin will continue to run in the background.

**WebAdmin URL**
This is the URL that WorldClient will use internally when users click the Advanced Settings link to edit their account settings via WebAdmin. If you are running WebAdmin with the built-in web server, then leave this field blank. If you are using an alternate web server such as IIS, and you have configured WebAdmin to run at an alternate URL or IP address, then specify that URL here.

**Bind WebAdmin's web server to these IPs only**
If you wish to restrict the WebAdmin server to only certain IP addresses, specify those addresses here separated by commas. If you leave this field blank then WebAdmin will monitor all IP Addresses that you have designated for your Domains 108.

**Restart WebAdmin (required when port or IIS value changes)**
Click this button if you wish to restart the WebAdmin server. Note: when changing the port setting you must restart WebAdmin in order for the new setting to be recognized.

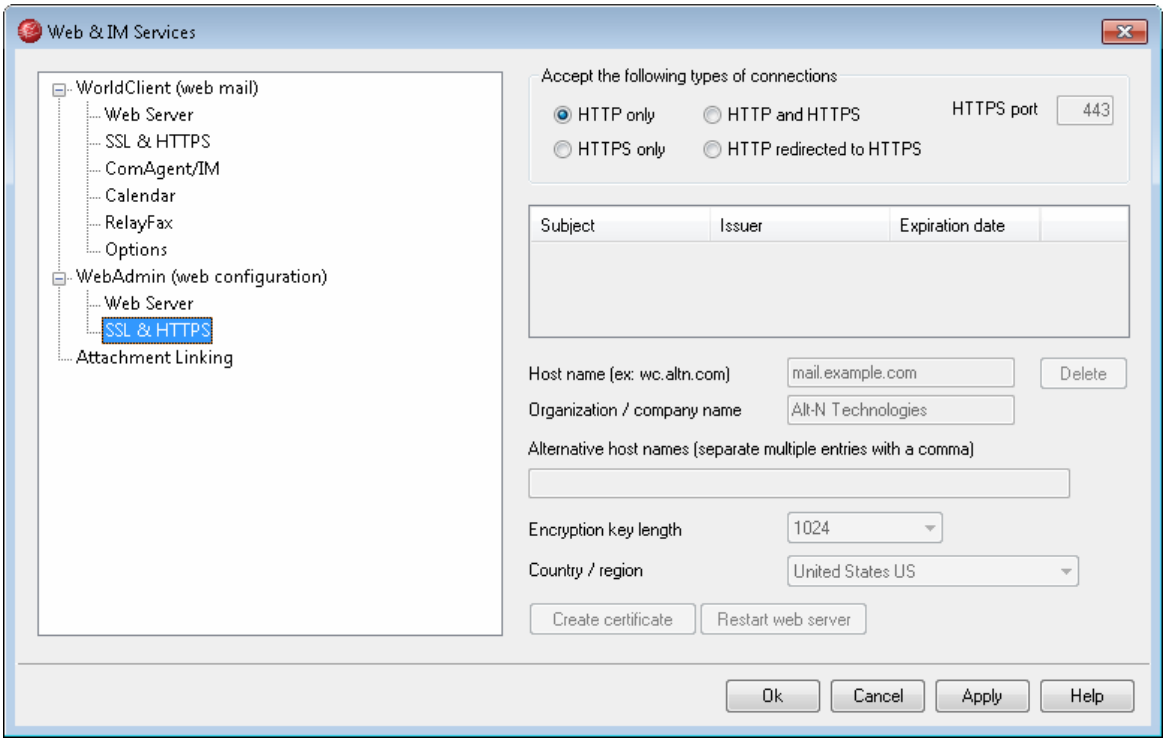
---

**See:**

**WebAdmin (web Configuration)** 132
**WebAdmin » HTTPS** 136
**Running WebAdmin under IIS** 138
**New Account Defaults » Web Services** 387
**Account Editor » Web Services** 346

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.3.2.2 SSL & HTTPS




MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WebAdmin to use HTTPS are located on the SSL & HTTPS screen under "Setup » Web & IM Services » WebAdmin (web configuration)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WebAdmin".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 309

This screen only applies to WebAdmin when using MDaemon's built-in web server. If you configure WebAdmin to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

#### Accept the following types of connections

**HTTP only**
Choose this option if you do not wish to allow any HTTPS connections to WebAdmin.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Only HTTP connections will be accepted.

**HTTP and HTTPS**
Choose this option if you want to enable SSL support within WebAdmin, but do not wish to force your WebAdmin users to use HTTPS. WebAdmin will listen for connections on the *HTTPS port* designated below, but it will still respond to normal http connections on the WebAdmin TCP port designated on the Web Server 134 screen of WebAdmin (web configuration).

**HTTPS only**
Choose this option if you wish to require HTTPS when connecting to WebAdmin. WebAdmin will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

**HTTP redirects to HTTPS**
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

**HTTPS port**
This is the TCP port that WebAdmin will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WebAdmin's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WebAdmin port that is designated on the Web Server 134 screen of WebAdmin (web configuration). If you are still allowing HTTP connections to WebAdmin then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

### Certificates

This box displays your SSL certificates. Single-click a certificate in this list to designate it as the certificate that you wish WebAdmin to use. Double-click a certificate to open it in the Certificate dialog to review its details or edit it.

MDaemon does not support multiple certificates for WebAdmin. All domains must share a single certificate. If you have more than one domain then enter those domain names (and any others that you wish to use to access WebAdmin) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

**Delete**
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Host name**
When creating a certificate, enter the host name to which your users will connect (for example, "wa.example.com").

**Organization/company name**
Enter the organization or company that "owns" the certificate here.

**Alternative host names (separate multiple entries with a comma)**
MDaemon does not support multiple certificates — all domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

**Encryption key length**
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

**Country/region**
Choose the country or region in which your server resides.

**Create Certificate**
After entering the information into the above controls, click this button to create your certificate.

**Restart web server**
Click this button to restart the web server. The web server must be started before new certificates will be used.

---

**For more information on SSL and Certificates, see:**

**Running WebAdmin under IIS** 138
**SSL and Certificates** 309
**Creating and Using SSL Certificates** 320

---

**For more information on WebAdmin, see:**

**Remote Configuration** 132
**WebAdmin » Web Server** 134
**New Account Defaults » Web Services** 387
**Account Editor » Web Services** 346

### 4.3.2.3 Running WebAdmin under IIS

WebAdmin is equipped with a built-in web server and therefore doesn't require Internet Information Server (IIS) to operate. However, it does support IIS, and can therefore

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

function as an ISAPI DLL.

**To configure to operate under IIS 5:**

1. Stop WebAdmin from running. You can do this by right-clicking on the WebAdmin entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.

2. Open the IIS management program (**Start→ Settings→ Control Panel→ Administrative Tools → Internet Services Manager**).

3. Right-click **Default Website** and then select **New→ Virtual Directory**.

4. Follow the Wizard as it takes you through the steps of creating a Virtual Directory. The following are suggested names and locations for data to be typed into the Wizard, but will vary depending on your installation of MDaemon and the location of WebAdmin.

   a. Alias: "`WebAdmin`". Click **Next**.
   b. Directory: "`c:\mdaemon\webadmin\templates`". Click **Next**.
   c. Click **Next**.
   d. Click **Finish**.

5. Set the Execute Permissions to **Scripts Only**.

6. Set the Application Protection to **Low (IIS Process)**.

7. Click the **Configuration** button in the Application Settings section of the Virtual Directory tab.

8. On the **Mappings** tab click the **Add**.

9. In the **Executable** field enter "`c:\mdaemon\webadmin\templates\WebAdmin.dll`". Note: This field cannot contain any spaces. If the path contains a space it must be converted to 8.3 format. The `dir /x` command will show the 8.3 name for a file or directory.

10. In the **Extension** field enter "`.wdm`" and select the radio button for **All Verbs**.

11. Click the **Script Engine** box.

12. Click **OK**.

13. All other mappings can be removed if you choose, then click the **OK**.

14. On the **Documents** tab add `login.wdm` as a Default Document and remove all other entries from the list.

15. In MDaemon, go to **Setup→ Web & IM Services→ WebAdmin** and click **WebAdmin runs using external web server**.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

16. In **WebAdmin URL** type "/WebAdmin/login.wdm".
17. Click **OK**.

### To configure to operate under IIS 6:

**Create a new application pool for WebAdmin:**

1. Stop WebAdmin from running. You can do this by right-clicking on the WebAdmin entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.
2. Open the IIS management program (**Start→ Settings→ Control Panel→ Administrative Tools →Internet Services Manager**).
3. Right-click **Application Pools**.
4. Click **New→ Application Pool**.
5. In the Application pool ID field type "Alt-N" and click **OK**.
6. Right-click **Alt-N**
7. Click **Properties**.
8. Click **Performance** tab.
9. Clear "**Shutdown worker processes after being idle for**" and "**Limit the kernel request queue**".
10. Click **Identity** tab.
11. In the drop-down for Predefined, choose **Local System**.
12. Click **OK**.

**Create a virtual directory for WebAdmin:**

1. Open the IIS management program (**Start→ Settings→ Control Panel→** Administrative Tools (Internet Services Manager).
2. Right-click your w eb site and then select New (Virtual Directory.
3. Specify and alias for the virtual directory (for example, "WebAdmin).
4. In the Path field, type the path to the WebAdmin Templates directory — for example, "C:\Program Files\Alt-N Technologies\WebAdmin\Templates".
5. Leave the Read and Run Scripts options checked.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

6. Finish the w izard and right-click on the Virtual Directory that w as created.
7. Select Properties.
8. On the Home Directory tab change the application pool to Alt-N.
9. Click the Configuration button.
10. Click Add to add an ISAPI extension mapping.
11. In the Executable field enter the path to the WebAdmin.dll file. For example, "C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll".
12. In the Extension field enter ".w dm"
13. Click the boxes for **Script Engine** and **Verify the file exists**.
14. Click **OK**.
15. All other mappings can be removed if you choose, then click the **OK**.
16. Select the **Documents** tab.
17. Ensure that **Enable default content page** is checked.
18. Ensure that only "`login.wdm`" exists in the list.
19. Click the **Ok** and exit the virtual directory properties dialog.

**Add `.WDM` to list of allowed web extensions:**

1. Click on the **Web Service Extensions** folder (in the IIS MMC).
2. Click **Add new web service extension**.
3. In the Extension name field enter "`WebAdmin`".
4. Click **Add** and then browse to the WebAdmin ISAPI extension. For example: `C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`.
5. Check **Set extension status to allowed**.
6. Click **OK**.
7. In MDaemon, go to **Setup→Web & IM Services→WebAdmin** and click **WebAdmin runs using external web server**.
8. In **WebAdmin URL** type "`/WebAdmin/login.wdm`".

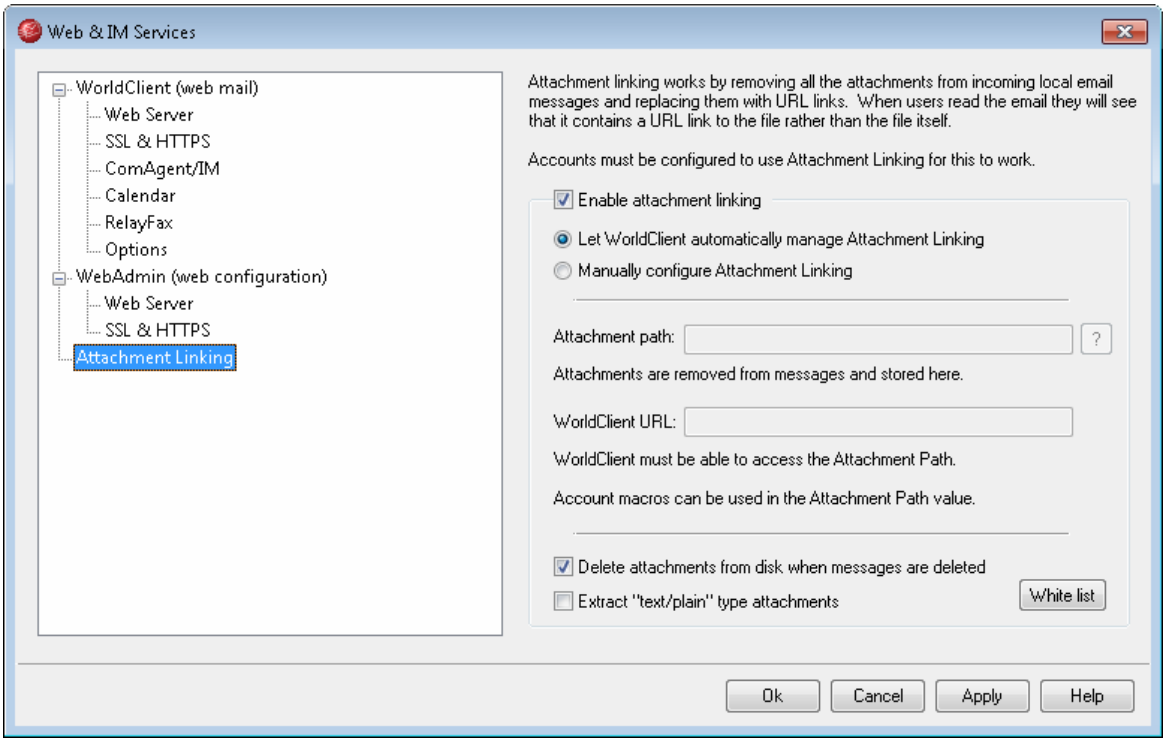
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

9. Click **OK**.

**For more information on WebAdmin, see:**

**Remote Configuration** 132
**WebAdmin » Web Server** 134
**WebAdmin » HTTPS** 136
**New Account Defaults » Web Services** 387
**Account Editor » Web Services** 346

### 4.3.3 Attachment Linking




Attachment Linking (Setup » Web & IM Services » Attachment Linking) is a feature that makes it possible for MDaemon to remove all attachments from incoming email messages, store them in a designated location, and then place URL links to the files in each message from which they are extracted. The recipients can then click those links to download the files. This can greatly speed up mail processing when your users retrieve their messages or synchronize their mail folders, since the messages will be devoid of large attachments. It can also provide increased security and an increased level of protection for your users, because attachments can be stored in a central location for monitoring by the administrator and will not be downloaded automatically to mail clients where they might be executed automatically. Further, if you choose the "*Let WorldClient automatically manage Attachment Linking*" option, management of the file locations and the WorldClient URL is handled automatically. If you choose to manage Attachment Linking manually, you can specify the location where the files will

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

be stored, and you can use special macros to make the location dynamic. In order for Attachment Linking to work, it must be enabled globally using the option on this screen, and each Account that you wish to use it must be configured specifically to do so on the Folder, Attachments, Groups 349 screen of the Account Editor. Finally, the links to the attachments that MDaemon will place in messages do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file.

**Enable attachment linking**
Click this checkbox to enable Attachment Linking for all accounts that are specifically configured to use it on the Folder, Attachments, Groups 349 screen of the Account Editor. When you enable this global option you will be asked if you also wish to enable the account specific option for all MDaemon accounts. If you choose "Yes" then Attachment Linking will be enabled for all accounts, and the corresponding option under New Account Defaults 380 will also be enabled. If you choose "No" then the Attachment Linking feature will be enabled but the account specific option will not—you must manually activate it for each account that you wish to use it. When Attachment Linking is enabled, the WorldClient server must remain active.

**Let WorldClient automatically manage Attachment Linking**
This is the default option when Attachment Linking is enabled. Use this option if you wish to let WorldClient handle Attachment Linking automatically. Extracted files will be stored at: "`...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\`".

**Manually configure Attachment Linking**
Choose this option if you wish to designate the folder in which extracted file attachments will be stored. You must designate both the attachment path and the WorldClient URL when you choose this option.

**Attachment path**
Use this text box to designate the folder in which to store extracted file attachments. You can set a static file path or use template 383 and script 393 macros to make the path dynamic. For example, "`$ROOTDIR$\Attachments\$DOMAIN$\`" will group all attachments into a subfolder named for the domain to which the user belongs, under a subfolder called "`Attachments`" contained in MDaemon's root folder (usually `C:\MDaemon\`). So, for "`user1@example.com`" the above example would cause the extracted attachments to be placed in the subfolder, "`C:\MDaemon\Attachments\example.com\`." You could further subdivide attachment storage by appending the "`$MAILBOX$`" template macro to the above example. This would cause user1's files to be stored in a subfolder beneath "`\example.com\`" called "`user1`." Therefore the new file path would be: "`C:\MDaemon\Attachments\example.com\user1\`."

**WorldClient URL**
Enter WorldClient's URL here (e.g. "`http://mail.example.com:3000/WorldClient.dll`"). MDaemon will use this URL when inserting the links to extracted attachments in messages.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Delete attachments from disk when messages are deleted**
Click this option if you want extracted attachments to be deleted from the server whenever the message to which they are linked is deleted. Give this option careful consideration before enabling it, because if it is enabled and a user collects his email via a POP3 client that is not configured to leave messages on the server, then all of his extracted attachments will be irretrievably lost. If this option is **not** enabled then no attachments will be lost, but a great deal of your hard drive space could eventually be taken up by outdated and useless files that their original recipient no longer wants or needs. Virtually all POP clients have the ability to leave messages on the server.

**Extract "text/plain" type attachments**
By default, `text/plain` attachment types will not be extracted. Click this checkbox if you wish to include those types in automatic extraction.

**White List**
Click this button to open the Attachment Linking white list. Include any file names that you do not wish to extract from messages. `Winmail.dat` is included on this list by default.

---

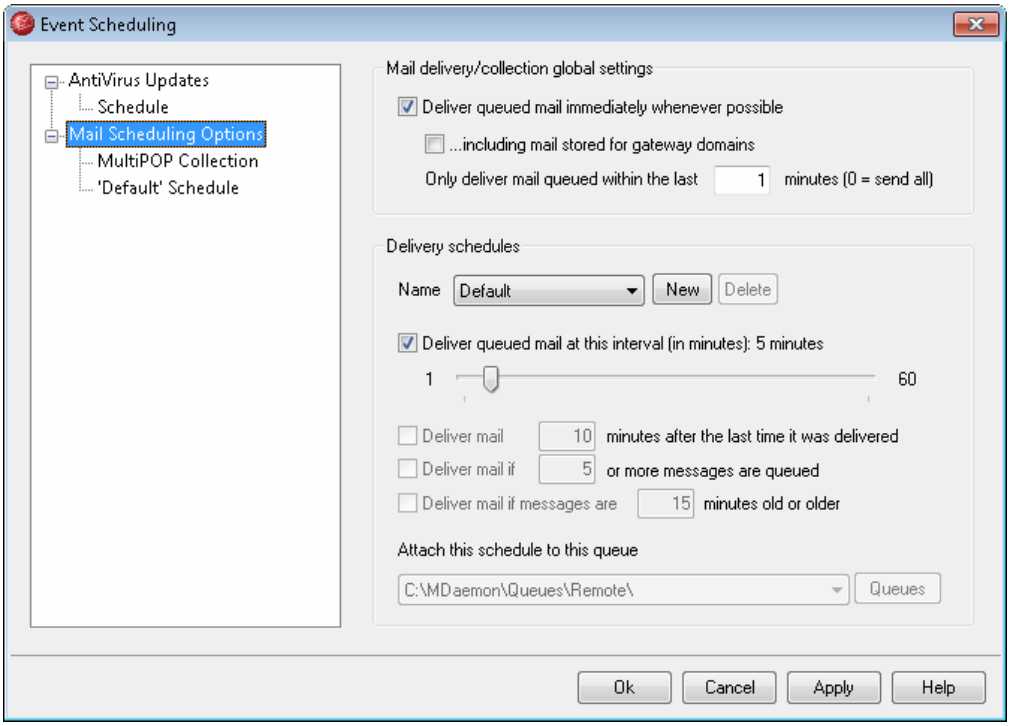
**See:**

**Folder, Attachments, Groups** 349
**Template Macros** 383
**Script Macros** 393

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# 4.4 Event Scheduling

## 4.4.1 Mail Scheduling Options




Click Setup » Default Domains/Servers » Event Scheduling to open MDaemon's Event Scheduler. The Mail Scheduling Options section of this dialog makes it possible for you to schedule MDaemon's Remote mail processing events as extensively or as simply as you prefer. You can use a counter to process mail at regular intervals, or you can schedule exact times for mail delivery and collection using the Mail Schedule 148 screens. You can also set conditions that will trigger mail processing at unscheduled times such as when a certain number of messages are waiting to be delivered, or when a message has been waiting a specified amount of time. Further, you can create custom schedules that you can assign to custom remote mail queues. Custom schedules make it possible for you to set different schedules for different types of messages. For example, you could create schedules for large messages, mailing list messages, certain domains, and so on.

If you have installed SecurityPlus for MDaemon 210, use the AntiVirus Updates 151 section of the Event Scheduler to schedule how often MDaemon will check for AntiVirus updates.

### Mail Delivery/Collection Global Settings

**Deliver queued mail immediately whenever possible**
When this option is enabled and a message arrives and is queued for remote delivery, rather than waiting for the next scheduled processing interval or some other event to trigger mail processing, MDaemon will immediately process and deliver

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

all remote mail that has been queued within the number of minutes designated in the *Only deliver mail queued within the last [xx] minutes* option below.

**...including mail stored for gateway domains**
Click this check box if you also want messages for Domain Gateways to be delivered immediately. However, this only applies to gateways with the *Deliver stored messages each time MDaemon processes remote mail* option enabled on the Gateway 460 screen of the Gateway Editor.

**Only deliver mail queued within the last [xx] minutes (0=send all)**
This option governs how recently messages must have been queued before the *Deliver queued mail immediately whenever possible* option above will spool them for delivery. When that option triggers remote mail processing, instead of attempting to deliver everything in the queue, MDaemon will process only those messages that were queued within the designated number of minutes. The entire queue will still be processed, however, when the *Process...queue* toolbar button is pressed or when any other normal scheduling event triggers remote mail processing. By default, this option is set to one minute. You can set it to "0" if you wish to process the entire queue every time remote mail processing is triggered, but that is not recommended since it is much less efficient.

The above options only apply to the Default schedule. They are unavailable for custom schedules (see the *Name...* option below).

**Name...**
Use this drop-down list box to select a schedule to edit. The Default schedule will always be used for the regular, remote mail queue and for DomainPOP and MultiPOP collected mail. For configurations using dialup services, the Default schedule will also be used for LAN Domains, which are remote domains that you have designated as residing on your local area network and therefore do not require RAS dialup. Other schedules can be assigned to custom remote mail queues, and messages can be routed to those custom queues 486 automatically by using the Content Filter 212. When you are finished editing a schedule's options, click OK or select another schedule for editing. If you make changes to a schedule and then select another schedule, a confirmation box will open asking you whether you wish to save or discard the currently selected schedule's changes before switching to the other schedule.

**New**
Click this option to create a new schedule. A box will open so that you can designate a name for it. After the schedule's name is designated, a corresponding Mail Schedule 148 screen will be created for it in the menu on the left. Use that screen to assign times to that schedule.

**Delete**
To delete a custom schedule, first select it in the *Name...* drop-down list and then click *Delete*. A confirmation box will open asking you if you are sure you wish to delete it. Deleting a custom schedule will not delete any custom remote queue or content filter rules associated with it. However, if you delete a custom queue then

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

any schedules associated with that queue will also be deleted, and all associated content filter rules as well.

**Deliver queued mail at this interval (in minutes)**
Click the check box and slide this bar left or right to specify the time interval between mail processing sessions. It can be configured to count down from a range of 1 to 60 minutes. After that amount of time, MDaemon will process remote mail before beginning the countdown again. When this check box is cleared, *Remote Mail* processing intervals will be determined by the other scheduling options.

**Deliver mail [xx] minutes after the last time it was delivered**
Use this option when you want a remote mail processing session to occur at a regular time interval after the last session occurred, regardless of the trigger that initiated the session. Unlike the rigidly fixed intervals used when setting up specific times or when using the *Deliver queued mail at this interval* slide bar, this option's time interval will reset each time mail is processed.

**Deliver mail if [xx] or more messages are queued**
When this option is enabled, MDaemon will trigger a mail session whenever the number of messages waiting in the remote queue meets or exceeds the number that you specify here. These mail sessions are in addition to any other normally scheduled sessions.

**Deliver mail if messages are [xx] minutes old or older**
When this box is checked, MDaemon will trigger a mail session whenever a message has been waiting in the queue for the number of minutes specified. These sessions are in addition to any other normally scheduled sessions.

### Queues

**Attach this schedule to this queue**
Use this option to associate the selected schedule with a specific custom remote mail queue. You can then use the content filter to create rules that will place certain messages in that queue. For example, if wanted to schedule mailing list messages destined for remote addresses to be delivered at some specific time, then you could create a custom queue for those messages, create a rule to put all of them into your custom queue, and then create a custom schedule and assign it to that queue.

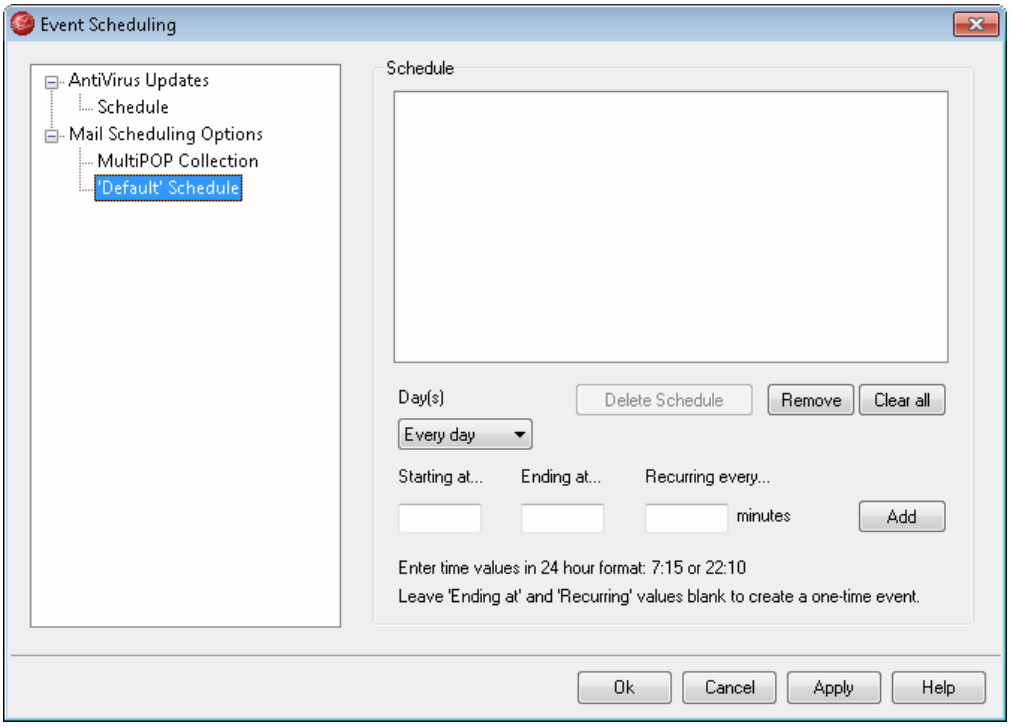
**Queues**
Click the button to open the Custom Queues 486 screen, on which you can create custom remote queues to use with the Event Scheduler.

**See:**

**Mail Schedule** 148
**AntiVirus Updates** 151

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.4.1.1 Mail Schedule




Each Mail Schedule corresponds to the schedule of the same name listed in the *Name* drop-down list on the Mail Scheduling Options 145 screen. Use each Mail Schedule to designate the specific times that remote mail processing will occur for that schedule. Mail Schedules are located at: Setup » Event Scheduling » Mail Scheduling Options » 'ScheduleName' Schedule.

#### Schedule

**Delete Schedule**
This button will delete the custom Mail Schedule. The schedule will be deleted and its entry will be removed from the *Name* drop-down list on the Mail Scheduling Options 145 screen. After you click this button, a confirmation box will open asking if you are sure you want to delete the schedule. This option is only available for custom schedules — the Default Schedule cannot be deleted.

**Remove**
To remove an entry from the list, select the entry and then click this button.

**Clear all**
This button removes all entries from the schedule.

#### Creating Schedule Events

**Day(s)**
When creating a new event for the schedule, first select the day or days on which this scheduling event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Starting at...**
Enter the time that you wish the event to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending at...* and *Recurring every...* options blank).

**Ending at...**
Enter the time that you wish the event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

**Recurring every [xx] minutes**
This is the time interval at which mail will be processed between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

**Add**
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

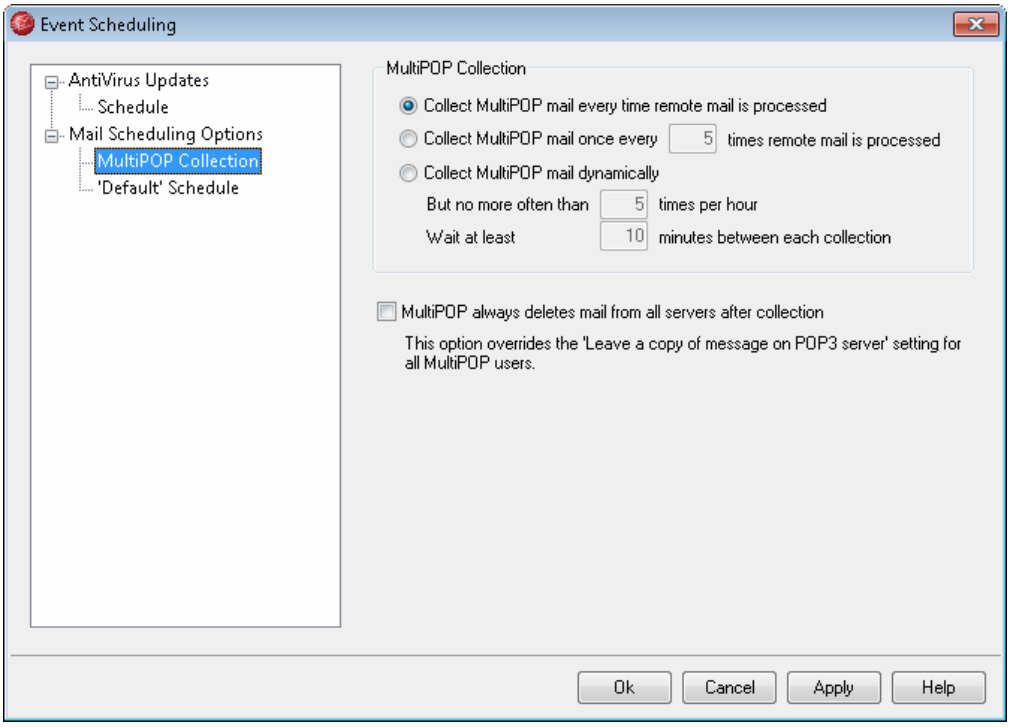
Depending on your needs, it may be sufficient to use the simple scheduling options on the Mail Scheduling Options 145 screen to control mail processing intervals. For example, it is pointless to make a specific schedule with events for every minute of every day when you can simply set the slider bar on Mail Scheduling Options to one minute intervals and accomplish the same thing. On the other hand, if you want the processing intervals to be more than an hour apart, or only on certain days, then you can use some combination of the scheduling options and mail specific times.

**See:**

**Mail Scheduling Options** 145
**AntiVirus Updates** 151
**AntiSpam Updates** 260

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.4.1.2 MultiPOP Collection




#### MultiPOP Collection

**Collect MultiPOP mail every time remote mail is processed**
Choose this option if you want MDaemon to collect all MultiPOP[369] mail every time that remote mail is processed.

**Collect MultiPOP mail once every XX times remote mail is processed**
Choose this option and specify a numeral in the box if you want MultiPOP mail to be collected less often than remote mail is processed. The numeral denotes how many times remote mail will be processed before MultiPOP mail will be collected.

**Collect MultiPOP mail dynamically**
Choose this option if you wish to collect MultiPOP messages dynamically. Ordinarily, MultiPOP is collected for all users at the same time at each remote mail processing interval, or at every *x* number of intervals. When collected dynamically, MultiPOP messages are collected for each individual user when that user checks his or her local mail via POP, IMAP, or WorldClient rather than for all users at once. However, because MultiPOP collection is triggered by a user checking his email, any new MultiPOP messages collected will not be visible to the user until he checks his mail *again*. Thus, he would need to check his mail twice in order to see new MultiPOP messages. The first time to trigger MultiPOP and a second time to see the mail that was collected.

**But no more often than XX times per hour**
In order to reduce the load that extensive use of MultiPOP can potentially place on your MDaemon, you can use this control to specify a maximum number of

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

times per hour that MultiPOP can be collected for each user.

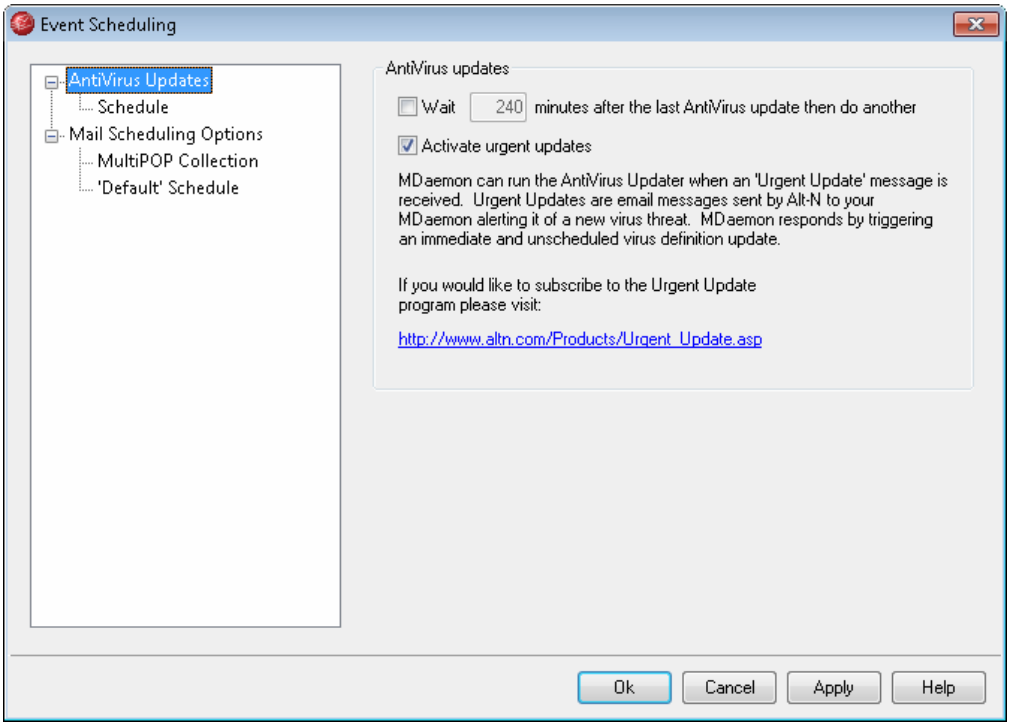
**Wait at least XX minutes between each collection**
This option can help to reduce the load on the mail server by limiting how frequently MultiPOP messages can be collected by each user. It will restrict MultiPOP mail collection to once every so many minutes per user. Specify the number of minutes that you wish to require the user to wait before being allowed to check MultiPOP again.

**MultiPOP always deletes mail from all servers after collection**
Click this check box if you wish to override the *Leave a copy of message on POP server* option (located on the MultiPOP 369 screen of the Account Editor) for all users. All messages will be deleted from each MultiPOP server after they are collected.

**See:**

**MultiPOP** 369

## 4.4.2 AntiVirus Updates




### AntiVirus Updates

**Wait XX minutes after the last AntiVirus update then do another**
Click this checkbox and specify the number of minutes that you want SecurityPlus for MDaemon to wait before checking for new virus signature updates. Note, this is actually the number of minutes that SecurityPlus for MDaemon will *attempt* to wait after the last time you checked for an update, whether the update was triggered by

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

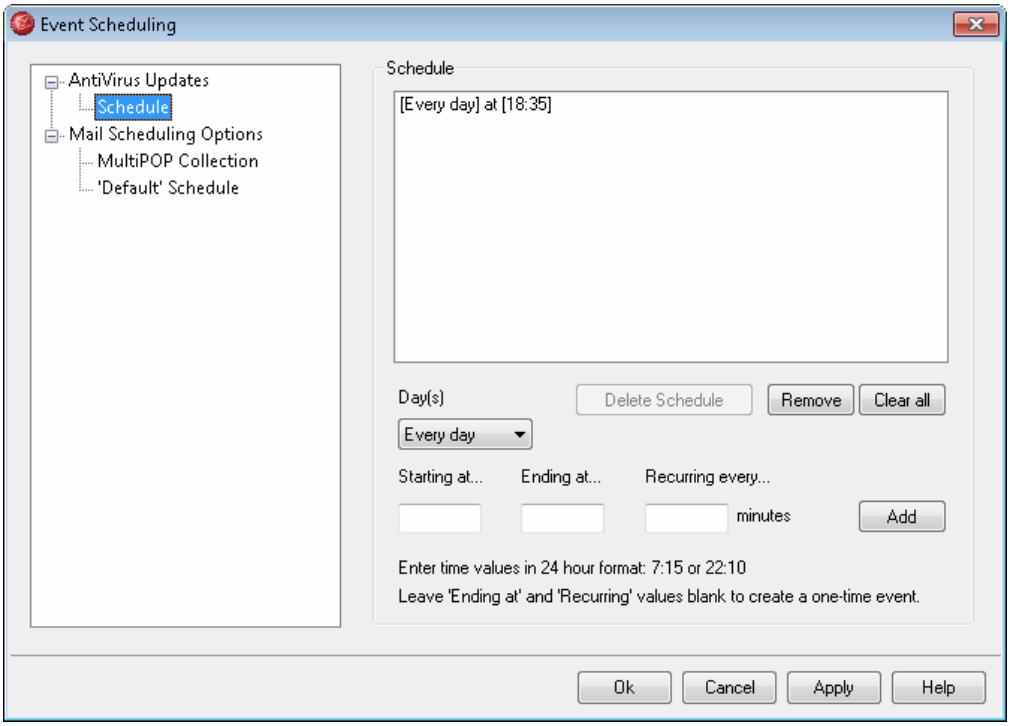
the scheduler or manually. The scheduler and manually triggered updates are given precedence over this setting and will therefore reset this counter if a SecurityPlus update event is triggered by one of those other methods. Thus, for example, if you have this option set to check for updates every 240 minutes and you manually check for an update after 100 minutes, this counter will be reset to 240.

### Urgent Updates

**Activate urgent updates**
Click this checkbox to activate the urgent updates feature. With this feature enabled, SecurityPlus for MDaemon will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message. To receive these messages you must add your domain to the Urgent Updates system at altn.com.

> You must have the "*Verify...DKIM signatures*" option on the DKIM Verification 285 screen enabled to use this feature.

## 4.4.2.1 AntiVirus Update Schedule




Use the AntiVirus Update Schedule to designate specific times for SecurityPlus 210 to check for AntiVirus updates. The schedule is located at: Setup » Event Scheduling » AntiVirus Updates » Schedule.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## Schedule

**Remove**
To remove an event from the list, select the entry and then click this button.

**Clear all**
This button removes all entries from the schedule.

## Creating Schedule Events

**Day(s)**
When creating a new event for the schedule, first select the day or days on which this scheduled update check event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

**Starting at...**
Enter the time that you wish the update check to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending at...* and *Recurring every...* options blank).

**Ending at...**
Enter the time that you wish the update check event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

**Recurring every [xx] minutes**
This is the time interval at which SecurityPlus will check for updates between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

**Add**
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

**See:**

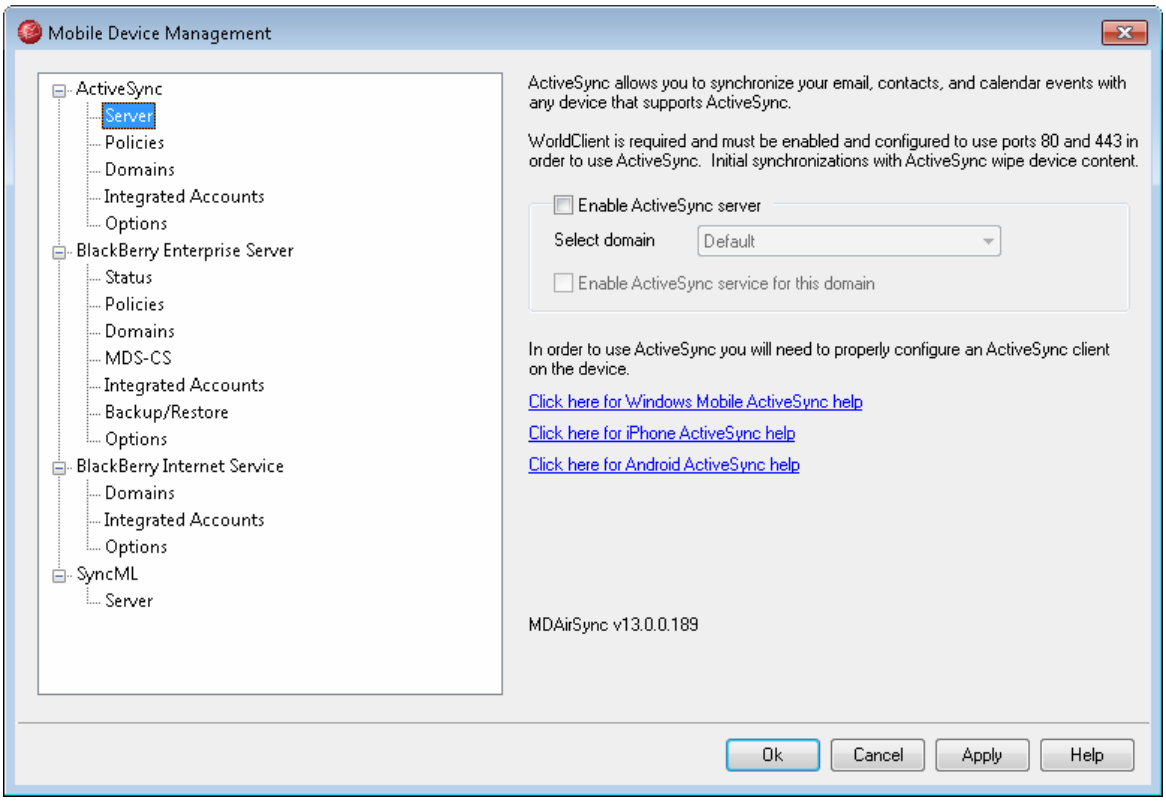
**AntiVirus Updates** 231
**AntiVirus** 231
**AntiVirus Updater** 233

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# 4.5 Mobile Device Management

## 4.5.1 ActiveSync

### 4.5.1.1 Server




MDaemon includes support for "ActiveSync for MDaemon," which is a separately licensed over-the-air (OTA) ActiveSync server. This server is capable of synchronizing a user's Email, default Contacts, default Calendar, and Tasks between his MDaemon/ WorldClient account and an ActiveSync capable device. MDaemon's ActiveSync options are located under: Setup » Mobile Device Management... » ActiveSync. There are also user-specific options located on the Account Editor's ActiveSync 355 and Options 377 screens.

If you enable ActiveSync for MDaemon the first time using a trial key, it will operate for 60 days. After that there is a one-time license fee if you wish to continue using it. You can acquire a license key from www.altn.com or your local distributor/reseller.

ActiveSync is a web-service extension that only works on ports **80** (for http) and **443** (for https). This is an ActiveSync implementation requirement. If ActiveSync is enabled and you are using WorldClient's built-in web server 116 but it is not running on port 80 or 443, then it will automatically begin running on port 80 in addition to whatever other ports you have configured on the Web Server 116 and SSL & HTTPS 121 screens. If you are using another server for WorldClient such as IIS then you must manually configure it to use port 80 or 443.

If you intend to run ActiveSync under IIS you must call the ActiveSync DLL (

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

MDAirSync.dll) when "/Microsoft-Server-ActiveSync" is requested. This is the request that all the ActiveSync clients will use. Some versions of IIS do not have this capability without downloading, installing, and configuring third party software.

All first time syncs with ActiveSync are a one way sync from the server to the device. You will lose the data on the device when you sync with ActiveSync for the first time. This is an ActiveSync implementation requirement. Therefore, backup your device data before using ActiveSync for the first time. Most devices that support ActiveSync warn the user that "**all device data will be lost**," but some do not. Please handle ActiveSync with care.

### Enabling/Disabling ActiveSync

Click *Enable ActiveSync server* to turn on ActiveSync for MDaemon. Then you can use the options below to control whether or not it is available to all or some of your domains.

### Setting the Default ActiveSync State

You can choose whether or not you want ActiveSync support to be enabled or disabled for your domains by default. This is the state of ActiveSync for all domains whose setting you haven't specifically overridden. To set the default state for your domains:

1. Click **Enable ActiveSync server**.
2. In the *Select domain* drop-down list, click **Default**.
3. Click **Enable ActiveSync service for this domain** to enable ActiveSync for all domains by default. Uncheck the box if you want it to be disabled for all domains by default.

### Enabling/Disabling ActiveSync for Specific Domains

To set the ActiveSync state for a specific domain:

1. Click **Enable ActiveSync server**.
2. In the *Select domain* drop-down list, choose a domain.
3. Click **Enable ActiveSync service for this domain** if you wish to enable ActiveSync for the domain. Uncheck the box if you wish to disable ActiveSync for the domain.

In order to use ActiveSync you will need to properly configure an ActiveSync client on the user's device. For instructions on how to do this, follow the links on the ActiveSync dialog within MDaemon.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

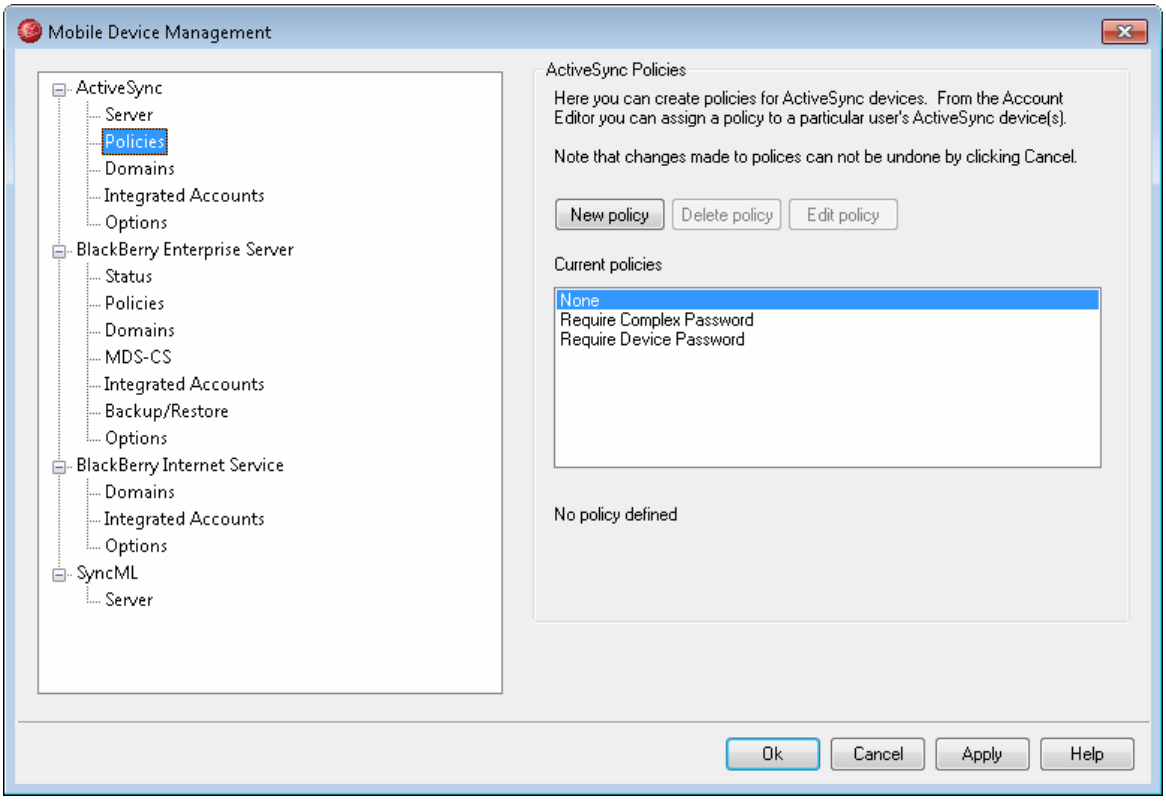
### ActiveSync Autodiscover Service

MDaemon supports the ActiveSync Autodiscover Service, which allows users to set up an ActiveSync account with just their email address and password, without needing to know the host name of the ActiveSync server. Autodiscover requires HTTPS[121] to be enabled, and for most systems it also requires that a new CNAME or A-record be added to DNS. "`autodiscover.<your-MDaemon-server>.com`" should resolve to the MDaemon server running ActiveSync (for example, `autodiscover.example.com`).

**See:**

**Account Editor » Options**[377]
**Web Server**[116]
**SSL & HTTPS**[121]

## 4.5.1.2 Policies




Use this screen to manage your ActiveSync device policies. Predefined policies are provided, and you can create, edit and delete your own policies. A default policy can be assigned per domain from the ActiveSync » Domains[159] screen. Policies can also be assigned per device, from the Account Editor's ActiveSync[355] screen.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies altogether and others may require a device reboot before changes take effect. Further, no policy is applied until the next time the device connects on its own to the ActiveSync server.

### ActiveSync Policies

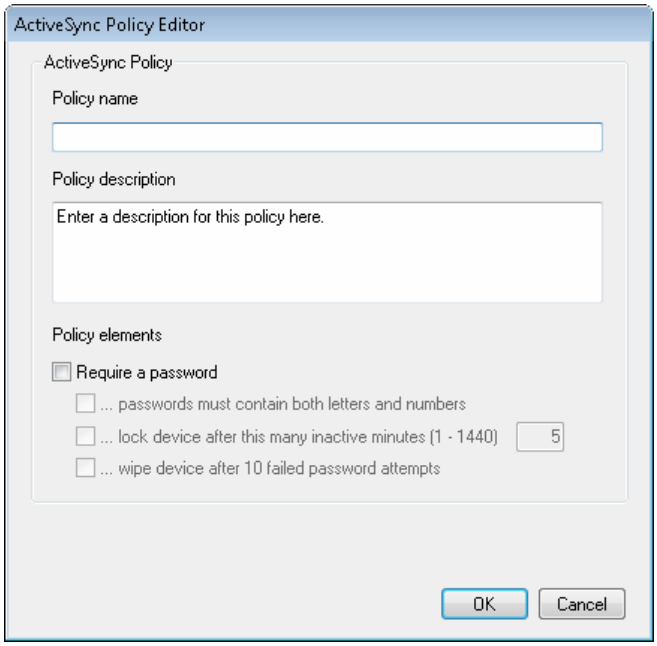
**New policy**
Click this button to open the ActiveSync Policy Editor[157], used for creating and editing your policies.

**Delete Policy**
To delete a policy, select a custom policy from *Current Policies* and then click *Delete Policy*. Click **Yes** to confirm your decision to delete the policy. The predefined policies cannot be deleted.

**Edit Policy**
To edit a policy, select a custom policy from *Current Policies* and then click *Edit Policy*. After making your desired changes in the policy editor, click **OK**. The predefined policies cannot be edited.

**Current Policies**
This area lists all predefined and custom made polices. When you select one of the policies, its *Policy description* will appear in the area below the list.

## ActiveSync Policy Editor




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## ActiveSync Policy

**Policy name**
Specify a name for your custom policy here.

**Policy description**
Use this area to describe your custom policy. This description appears below the *Current Policies* list when you select the policy.

## Policy Elements

**Require a password**
Include this policy element to force the ActiveSync device to require a password and to enable selection of other policy elements which require a password to be present.

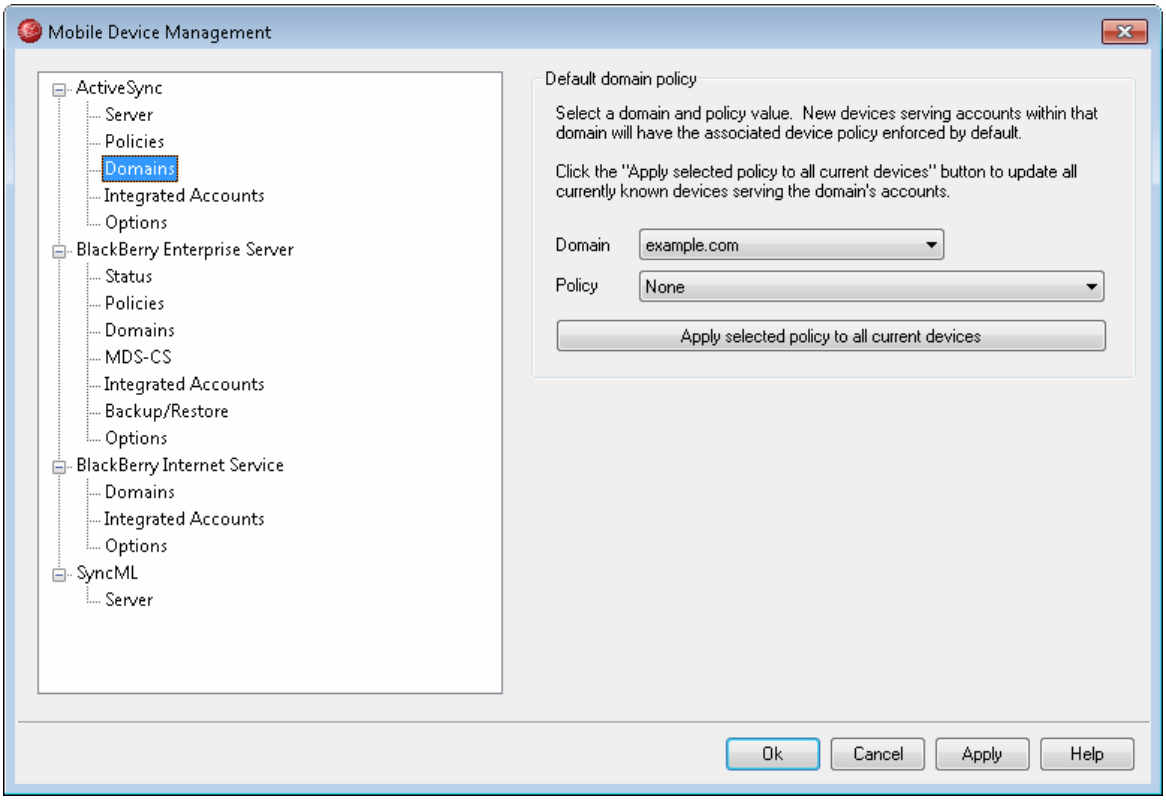
**...passwords must contain both letters and numbers**
Include this policy element to force a more complex form for ActiveSync device passwords (requires "Require a password" policy element enabled).

**...lock device after this many inactive minutes (1-1440)**
Include this policy element to force the device to lock the screen after a given number of inactive minutes, from 1-1440. This is the maximum number of inactive minutes that a device can wait before being locked, therefore a user could set his or her device to lock sooner than this value.

**...wipe device after 10 failed password attempts**
Include this policy element to wipe all device content (return to factory install settings) following 10 consecutive failed password attempts. For more information on wiping an ActiveSync device, see: ActiveSync » Integrated Accounts 160 .

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.5.1.3 Domains




Use this screen to assign the default ActiveSync policy 156 for each of your domains. If you wish to assign a different policy for a specific account's device, you can do so from the Account Editor's ActiveSync 355 screen.

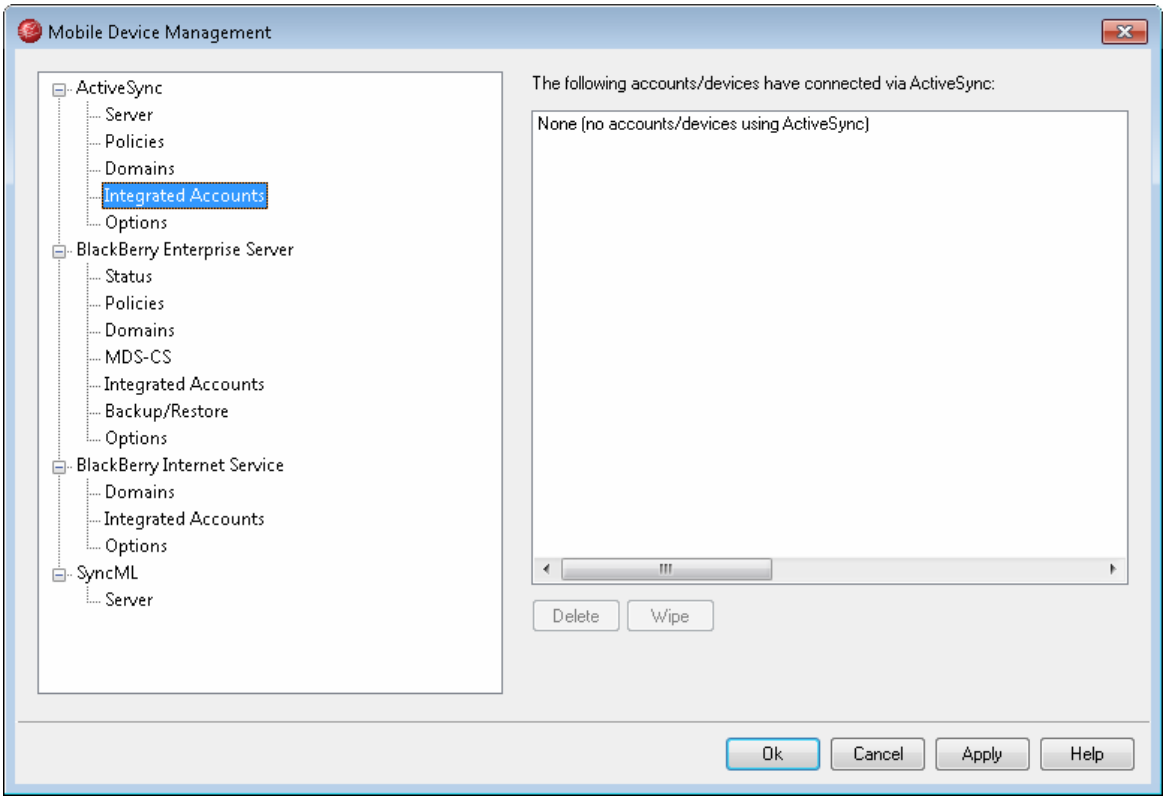
#### Assigning a Default ActiveSync Policy

To assign a default ActiveSync policy to your domains:

1. Select a domain from the Domain drop-down list.
2. From the Policy drop-down list, choose the policy that you wish to assign.
3. If you wish to apply the selected policy to all ActiveSync devices that are already associated with the domain, click **Apply selected policy to all current devices**. If you only wish to apply this policy to new devices, skip this step.
4. Click **OK** or **Apply**.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.5.1.4 Integrated Accounts




This screen contains an entry for each ActiveSync device associated with your system. Double-click any entry to see more details about the device.

#### Deleting an ActiveSync Device

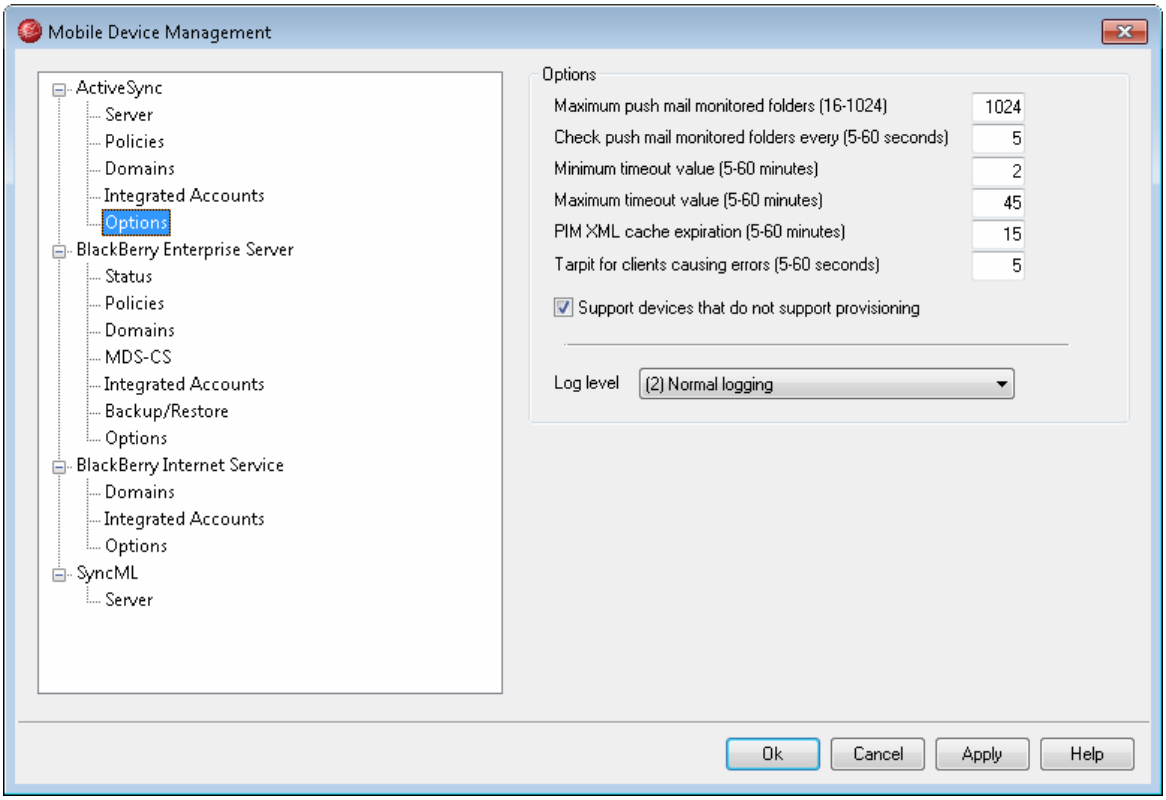
When you select an ActiveSync device from the list and click *Delete*, this will remove the device from the list and delete all synchronization data related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same device, MDaemon will treat the device as if it had never before been used on the server; all device data will have to be re-synchronized with MDaemon.

#### Remotely Wiping an ActiveSync Device

When you select an ActiveSync device from the list and click *Wipe*, the next time the device connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the device, this may remove everything on it, including downloaded apps. Further, as long as the device's ActiveSync entry exists in MDaemon, it will be wiped again if it ever connects again to MDaemon in the future. If you no longer wish to wipe the device when it connects (for example, if a lost device is recovered and you wish to use it again with the account) then you must first use the *Delete* option above to remove the device from MDaemon.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.1.5 Options




**Options**

**Maximum push mail monitored folders (16-1024)**
This is the maximum number of mail folders for each ActiveSync device that MDaemon will monitor for push mail.

**Check push mail monitored folders every (5-60 seconds)**
This is how often MDaemon will check each monitored folder for new messages, to push to each ActiveSync device.

**Minimum timeout value (5-60 seconds)**
This is how long a Ping Request must be, at the minimum. It is the minimum time required before the request times out and another Ping Request should be issued from the client.

**Maximum timeout value (5-60 seconds)**
This is the maximum amount of time allowed before a Ping Request times out.

**PIM XML cache expiration (5-60 seconds)**
Contacts, Calendar and Tasks are cached to reduce the workload on the server. This is how long a user's data is cached after it is last accessed. The data is automatically reloaded if the data changes on disk.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Tarpit for clients causing errors (5-60 seconds)**
When a device is causing errors, MDaemon will intentionally delay that client's connections by this many seconds.

**Support devices that do not support provisioning**
Some devices do not respond to provisioning commands correctly, therefore not allowing security requirements to be set on them. Enable this option if you wish to allow those devices to connect anyway.

### Log Level

**ActiveSync Log Level**
ActiveSync for MDaemon supports six levels of logging, from *(1) Debug logging* to *(6) No logging*. Generally *(1) Debug logging* should only be used to diagnose problems. The *(2) Normal logging* setting provides a good level of data and is the default setting.

## 4.5.2 BlackBerry Enterprise Server

MDaemon Pro is equipped with a BlackBerry Enterprise Server, which makes it possible for your users to synchronize their MDaemon/WorldClient email, calendar, and other personal information management (PIM) data with their BlackBerry smartphones. BlackBerry platform support also makes it possible for you to set security polices for user devices and even erase a device should it be lost or stolen.

MDaemon's BlackBerry Enterprise Server features include:

- No need for third-party sync clients. Each user's data is synchronized using software already present on all BlackBerry devices.
- MDaemon/WorldClient email (including mail folders) is synchronized with the device in both directions. Therefore whether mail is read, moved, deleted, etc. on the device or the server it will be synchronized on both.
- Two-way Calendar synchronization. For example, if you create a new appointment, set a reminder, or modify an appointment on either the device or within WorldClient it will be synchronized in both places.
- Two-way tasks and notes synchronization.
- Global address book lookup.
- Scheduling with free/busy.
- Limited BlackBerry device policy support, so that you can set device policies such as: require passwords, expiring passwords, encrypt media files, and more.
- Set different policies for individual domains or users.
- Support for BlackBerry Balance. BlackBerry Balance allows for the separation of work and personal information on BlackBerry devices. BlackBerry Balance is only supported on BlackBerry devices running OS 6.0 MR2 or higher.
- Use the BlackBerry MDS Connection Service (MDS-CS) for behind-the-firewall

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

access to files and web applications from BlackBerry devices. This will, for example, allow you to access your private Intranet without a VPN connection.

- Remotely change the device's password and lock it.
- Erase all data from the device, for example if it is lost or stolen.
- Backup and Restore options for your BlackBerry Enterprise Server database.

MDaemon's main BlackBerry Enterprise Server options are located at: Setup » BlackBerry... » BlackBerry Enterprise Server, and the account-specific options are located on the BlackBerry Enterprise Server 351 screen of the Account Editor.

BlackBerry Enterprise Server is not available in some countries and regions.

## BlackBerry Dialog

The BlackBerry Enterprise Server section of the BlackBerry dialog has the following screens:

**Status** 166 — You can enable/disable the BlackBerry Enterprise Server from this screen and see the status of its various components and services. Your unique Server Routing Protocol (SRP) information in also displayed here, including your SRP ID and Key.

**Policies** 167 — This screen is where you will create and manage the IT policies that you will assign to activated BlackBerry devices. Polices control various things such as whether or not the device must be secured by a password or its files encrypted.

**Domains** 174 — Use the options on this screen to choose the default policy that will be assigned to each domain's new accounts. You can also apply a policy to a domain's existing accounts.

**MDS-CS** 175 — The BlackBerry Mobile Data System Connection Service (MDS-CS) permits behind-the-firewall access to files and web applications from BlackBerry devices. It receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, and sends login requests so that users can view Internet and Intranet content on their BlackBerry devices.

**Integrated Accounts** 176 — This screen lists all BlackBerry enabled accounts and their current state: activated or not activated. Activated accounts also list the activated device's PIN. Further, there is a button on the bottom of the screen that you can use to initiate a slow sync of all activated accounts. This resynchronizes all account data, ensuring that the data on the devices matches the data in MDaemon.

**Backup/Restore** 177 — You can manually backup your BlackBerry Enterprise Server database from this screen and specify how many nightly backup files to save.

**Options** 179 — With this screen you can set the BlackBerry Enterprise Server services to stop when MDaemon stops, configure logging options, and set several synchronization options for email and calendar data.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## BlackBerry Device Activation

In order to begin using MDaemon's BlackBerry Enterprise Server features an account must "activate" a BlackBerry device with MDaemon. To do this complete the following steps.

**In MDaemon:**

1. Go to: Setup » BlackBerry... » BlackBerry Enterprise Server » Status.
2. Click **Enable BlackBerry Enterprise Server** if it is not already enabled.
3. If you need to create a custom policy for the device, click **Policies**167 in the left pane to do so.
4. Click **OK**.
5. Go to: Accounts » Account Manager..., and double-click the account that you wish to allow to activate a device.
6. Click **BlackBerry Enterprise Server**351 in the left pane of the Account Editor.
7. Click **Enable BlackBerry device synchronization**.
8. Choose a policy from the drop-down list.
9. Click **OK**.

**On the user's device:**

1. Disable or remove any third-party sync clients (such as a SyncML client) currently in use to synchronize data with the MDaemon account.
2. If the device is configured to use the BlackBerry Internet Service (BIS) to get email from the account, go to the device's email setup and remove that account.
3. If there are any existing calendar entries on the device, you must either wipe the device or reset the calendar. Otherwise existing calendar data on the MDaemon server may not be sent to the device. Always backup your device data before doing this. **Note:** if you choose to reset the calendar rather than wipe the device, the reset may be performed after activation. See **Resetting the Device Calendar**181 for more information.

**Note:** Failure to ensure that Steps 1 and 2 above are completed may result in duplicates of email, calendar entries, or other PIM data on the device.

**In WorldClient, the user must:**

1. Log in to WorldClient.
2. Go to: Options » BlackBerry Management.
3. Connect the device via a USB cable and follow the directions on the screen (requires Internet Explorer 6 or later).

   -or-

   Enter an activation password, click **Save**, and then activate the device over-

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the-air (OTA) directly from the device's Enterprise Activation screen — the user will enter the account's email address and activation password on the device. **Note:** Not all devices support OTA activation.

4. Sign out from WorldClient.

After initiating the activation process, whether via USB cable or OTA, it will continue on the device until finished. When the activation process is complete it will be paired with the MDaemon/WorldClient account. Within a short time data will begin to synchronize.

Depending on the device and operating system installed, activation may delete all data on the device, restoring it to its default settings before synchronizing it with MDaemon/ WorldClient. For this reason, before activating the device the user should use Desktop Manager or some other means to backup or export any data that he or she does not wish to lose.

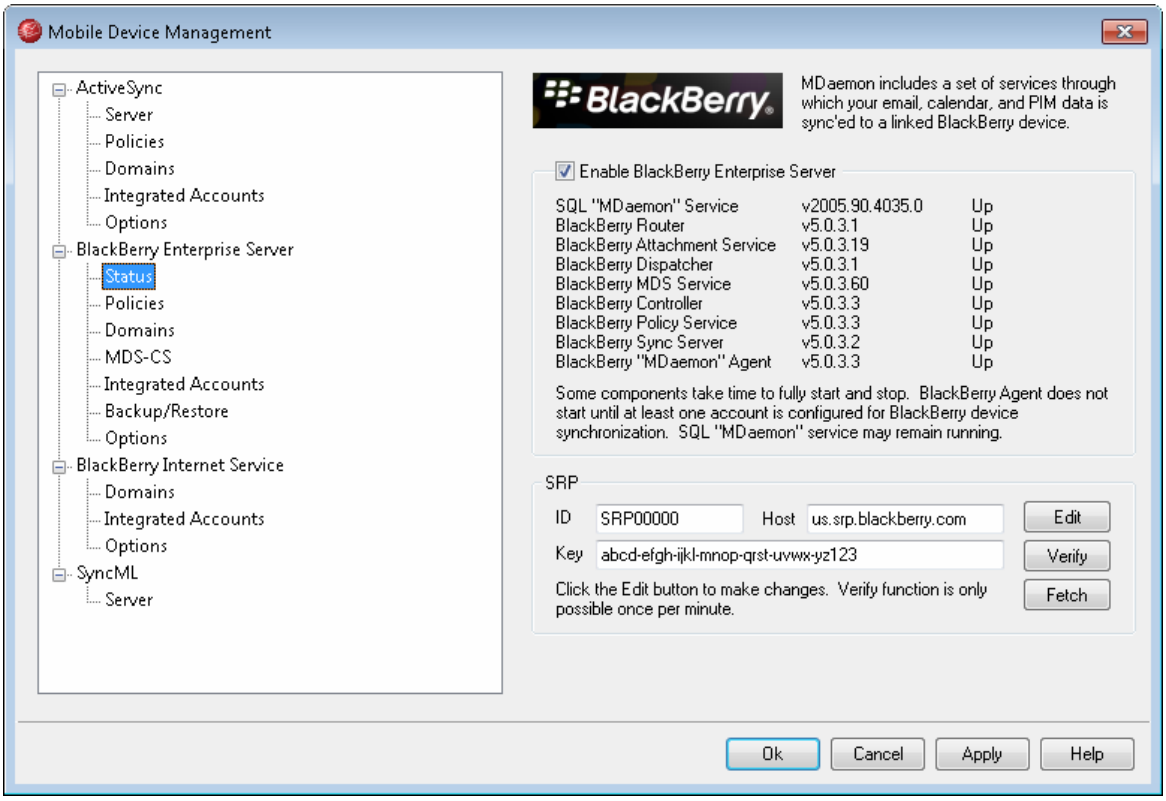
After a device is activated it may have various functionality changes or operating differences when compared to its state prior to BlackBerry Device Activation. The degree of difference depends on the device, OS, policy used, and whether or not it was previously activated on a different BlackBerry Enterprise Server.

**See:**

**Account Editor » BlackBerry Enterprise Server** 351
**BlackBerry Internet Service** 183

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.2.1 Status




This screen is located at: `Setup » BlackBerry... » BlackBerry Enterprise Server » Status`. It is used to enable or disable the BlackBerry Enterprise Server and displays the status of its various components and services. Your unique Server Routing Protocol (SRP) information in also displayed here, including your SRP ID and Key.

#### Enable BlackBerry Enterprise Server

Check this box to enable the BlackBerry Enterprise Server (BES), starting its various services. Some of these components may take time to fully start or stop, and the SQL "MDaemon" Service may continue running when the BlackBerry Enterprise Server is stopped. The BlackBerry "MDaemon" Agent will not start until at least one account is enabled for BlackBerry device synchronization[351].

#### SRP

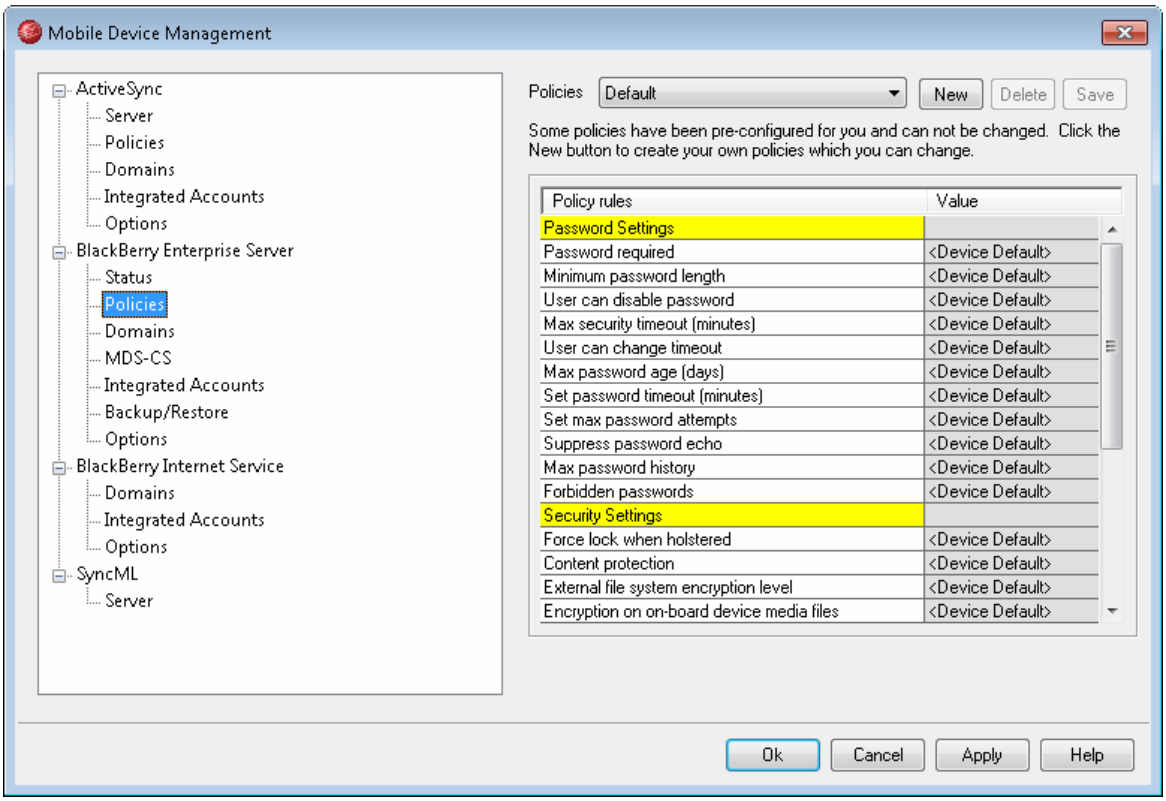
Server Routing Protocol (SRP) is used to authenticate and identify traffic between your MDaemon and your BlackBerry devices across the wireless network. This requires that your MDaemon have a unique SRP ID and SRP Key, which is obtained automatically during installation. Your SRP credentials are associated with your MDaemon server and cannot be used by any other server. You should not need to edit this information, but if it is necessary to do so then an **Edit** button is provided. You can also click **Verify** to confirm that your SRP credentials are valid.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**See:**

[BlackBerry Enterprise Server](#) 162
[Account Editor » BlackBerry Enterprise Server](#) 351

### 4.5.2.2 Policies




When a BlackBerry device is activated on MDaemon, a designated policy is pushed to that device. Policies are sets of rules that govern what is required or permitted on a device. They allow you to do things like require passwords, force the device to lock when holstered, encrypt files on the device, and more. Policies can be assigned to domains and to individual accounts. Use the Domains 174 screen to assign policies to domains, or use the BlackBerry Enterprise Server 351 screen on the Account Editor to assign them to specific accounts. MDaemon is equipped with three pre-configured policies, and you can create your own custom policies.

After a device is activated it may have various functionality changes or operating differences when compared to its state prior to BlackBerry Device Activation. The degree of difference depends on the device, OS, policy used, and whether or not it was previously activated on a different BlackBerry Enterprise Server.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## Pre-configured Policies

There are three pre-configured policies that cannot be edited or removed:

**Default**
This policy causes the BlackBerry device to use standard BlackBerry Enterprise Server defaults for all settings. This is a standard "out-of-the-box" and "under the control of a BlackBerry Enterprise Server" policy configuration.

**Password Required**
This policy is like *Default* except that it sets the *Password Required* rule to `YES` and the *User can disable password* rule to **No** (see rule descriptions below). Devices with this policy must be secured by a password.

**Expiring Passwords**
This policy is like *Password Required* but also sets the *Max password age (days)* rule to `30`. The password on the device will have to be changed at least every 30 days.

## Creating a Custom Policy

To create a custom policy:

1. Click **New**.
2. Enter a name for the policy.
3. Click **OK**.
4. Set the various policy rules as desired.
5. Click **Save**.

# Policy Rules

The following is a list of all policy rules that you can set when creating or editing a custom policy.

### Password Settings

Contains policy rules that apply to BlackBerry device password settings.

**Password required**
Specify whether the BlackBerry device requires a password. Set this rule to **YES** to require the user to enter a password to unlock the BlackBerry device.

Rule dependency: If you enable this rule, you should set the *User can disable password* rule to **NO** to prevent the BlackBerry device user from disabling this rule.

**Minimum password length**
Type the minimum required length, in characters, of the BlackBerry device password. This rule only controls the minimum password length, not the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

maximum password length. The maximum password length is 32 characters. The valid range for the value of this rule is 4 through 14.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

**User can disable password**
Specify whether the user can disable the requirement for a BlackBerry device password. Set this rule to **NO** to prevent users from disabling the password requirement on the BlackBerry device.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

**Max security timeout (minutes)**
Specify the maximum time, in minutes, that a BlackBerry device user can set as the security timeout value (the number of minutes of BlackBerry device user inactivity allowed before the security timeout occurs and the device requires the user to type the BlackBerry device password to unlock it). The BlackBerry device user can set any timeout value that is less than or equal to the maximum value, unless you set the *User can change timeout* rule value to **NO**. The maximum security timeout value available by default on the BlackBerry device is 60 minutes. The valid range for the value of this rule is **10-480** minutes.

**Note:** Use the *Set Password Timeout (minutes)* rule if you wish to set a specific timeout value.

Rule dependency: The BlackBerry device uses this policy rule only if the *Password required* rule is set to **YES**.

**User can change timeout**
Specify whether the BlackBerry device user can change the security timeout. If set to **YES**, the user can set the timeout to any available value up to the limit set in the *Max security timeout (minutes)* rule. Set this rule to **NO** if you wish to prevent the user from changing the timeout value. If no value is set then a default value of **YES** is used.

**Max password age (days)**
Type the number of days until a BlackBerry device password expires and the BlackBerry device prompts the user to set a new password. The valid range for the value of this rule is **0-65535** days. **Note:** Set this rule to **0** to prevent the BlackBerry device password from expiring.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Set password timeout (minutes)**
Specify the amount of time, in minutes, of BlackBerry device user inactivity allowed before the security timeout occurs and the BlackBerry device requires the user to type the password to unlock the BlackBerry device. The valid range for the value of this rule is **0-60**.

**Note:** The default security timeout interval is 2 minutes of inactivity for BlackBerry device software versions earlier than 4.7, and 30 minutes of inactivity for BlackBerry device software versions 4.7 and later.

Rule dependencies: The BlackBerry device uses this rule only if the *Password required* rule is set to **YES**. If you do not set the *User can change timeout* rule to **NO**, the BlackBerry device user can set the password timeout to one of a range of values. The maximum security timeout value available by default on the BlackBerry device is 60 minutes.

**Set max password attempts**
Set the number of password attempts (incorrect passwords entered) permitted on the BlackBerry device before the BlackBerry device data is erased and the BlackBerry device is disabled. The valid range for the value of this rule is **3-10** attempts. **10** attempts are allowed by default.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

**Suppress password echo**
Set this rule to **YES** to prevent the echoing (printing to the screen) of characters typed into the password screen after the user has entered a set number of incorrect passwords while attempting to unlock the device.

**Note:** You can use the *Set max password attempts* rule to designate the number of incorrect password attempts allowed before password echoing occur (if permitted).

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a password, set the *Password required* rule to **YES**.

**Max password history**
Set the maximum number of previous passwords against which the BlackBerry device can check new passwords to prevent reuse of the old passwords. The valid range for the value of this rule is **0-15** passwords. Set this rule to **0** to prevent the BlackBerry device from checking for reused passwords. If you do not set this rule, a default value of **0** will be used.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Forbidden passwords**
Type a list of comma-separated string values representing words that users are not permitted to use within their passwords.

**Note:** The BlackBerry device automatically prevents common letter substitutions. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa$zword", or "password123" on the BlackBerry device.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

## Security Settings

Contains policy rules that apply to BlackBerry device security."

**Force lock when holstered**
Specify whether the BlackBerry device is security locked when placed in the holster. If you do not set this rule, a default value of **NO** will be used.

**Content protection**
Specify whether content protection is turned on.

When content protection is turned on, BlackBerry device content is always protected with the 256 bit AES encryption algorithm. If the BlackBerry device is locked when it receives content, the BlackBerry device randomly generates the content protection key (a 256 bit AES encryption key) and an ECC key pair, derives an ephemeral 256 bit AES encryption key from the BlackBerry device password, and uses the ephemeral key to encrypt the content protection key and the ECC private key.

Rule dependency: The BlackBerry device uses this policy rule only if the *Password required* rule is set to **YES**.

**External file system encryption level**
Specify the level of file system encryption that the BlackBerry device uses to encrypt files that it stores on an external file system. You can use this policy rule to require the BlackBerry device to encrypt an external file system, either including or excluding multimedia directories. If you do not set this rule, a default value of **Level 0** (i.e. Not Required) will be used.

You can set this rule to the following values:

**Level 0:** Not Required

**Level 1:** Encrypt to User Password (excluding multi-media directories)

**Level 2:** Encrypt to User Password (including multi-media directories)

**Level 3:** Encrypt to Device Key (excluding multi-media directories)

**Level 4:** Encrypt to Device Key (including multi-media directories)

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Level 5:** Encrypt to User Password and Device Key (excluding multi-media directories)

**Level 6:** Encrypt to User Password and Device Key (including multi-media directories)

**Encryption on on-board device media files**
Specify whether the media files located on the on-board device memory will be encrypted to the user password and the device generated key if on-board device memory exists. If you set this rule to **Required** or **Disallowed** the user cannot change this setting on the device. If you do not set this rule, a default value of **Allowed** will be used.

Rule dependency: The BlackBerry device uses this policy rule only if the *Content protection strength* is set.

**Password required for application download**
Specify whether the BlackBerry device will prompt the user for their password prior to using the browser to download applications.

Rule dependency: The BlackBerry device uses this rule only if a BlackBerry device password is set. To require a BlackBerry device password, set the *Password required* rule to **YES**.

**Disable organizer data access for social networking apps**
This rule specifies whether a BlackBerry device must prevent social networking applications from accessing organizer data such as contacts and calendar data. Set this to **NO** to grant social networking applications access to the address book, calendar, and other organizer data. This rule's default value is **YES**, social networking applications cannot access organizer data on the device.

### BlackBerry Balance

Contains policies governing separation of work and personal data.

**Enable separation of work content**
Specify whether a BlackBerry device distinguishes between work data and personal data and whether the applications on the device can access work data.

If you do not set this rule, a default value of **NO** will be used.

**Disable forwarding of work content using personal channels**
Specify whether a BlackBerry device user can send work data to contacts using personal resources (for example, SMS text messaging, MMS messaging, or personal email accounts).

If you do not set this rule, a default value of **NO** will be used.

Rule dependency: This rule requires the *Enable separation of work* rule to be enabled.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Require work resources for conducting work activities**
Specify whether a BlackBerry device must use work resources (for example, work email accounts or work calendars) when a BlackBerry device user conducts work activity (for example, sending an email message to a work contact or scheduling a work appointment).

If you do not set this rule, a default value of **NO** will be used.

Rule dependency: This rule requires the *Enable separation of work* rule to be enabled.

**Work domains**
Type a list of comma-separated string values listing domain names that the BlackBerry device will identify as a work resource (for example: altn.com, example.com). Sub-domains are included automatically.

### Other

Miscellaneous settings

**Allow web-based software loading**
Specify whether to allow a user to update the BlackBerry device software using the web-based software loading feature. If you do not set this rule, a default value of **NO** will be used.

**MDS browser domains**
Specify a list of web addresses that the BlackBerry device should retrieve using the BlackBerry browser. Separate multiple web addresses with a comma. If you wish to allow the BlackBerry browser to retrieve sub-domains of a web address then prefix the domain with a period. For example, type "`.example.com`" to allow for sub-domains of `example.com`, such as: `mail.example.com`, `www.example.com`, etc.

This rule applies only to Java-based BlackBerry devices version 4.2.0 and higher.

**Policy author's name**
Enter the name of the author of this policy.

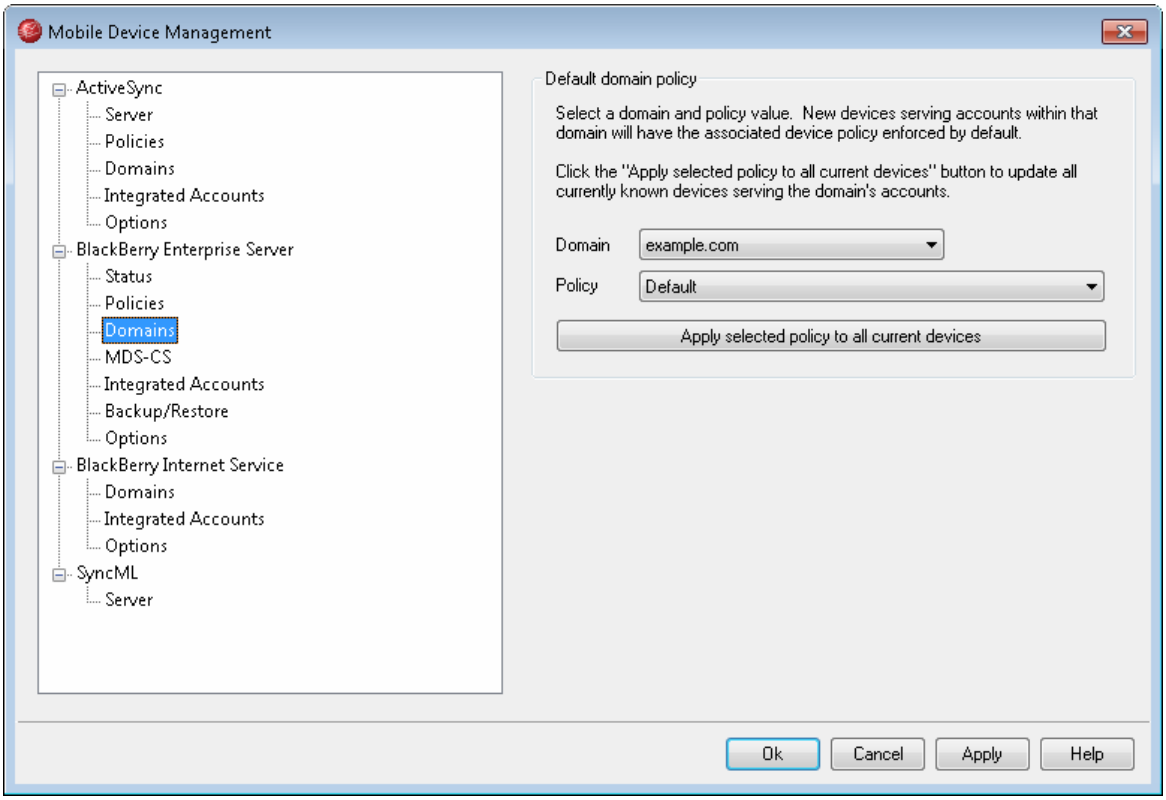
**Policy description**
Enter some text to describe this policy.

**See:**

**BlackBerry Enterprise Server** 162
**Domains** 174
**Account Editor » BlackBerry Enterprise Server** 351

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.2.3 Domains




#### Default Domain Policy

To designate the default policy[167] that will be assigned to each new BlackBerry activation on a particular domain, select the desired domain from the drop-down list, select the policy that you wish to assign to all new activations, and then click **OK**. Only new activations will have this policy assigned. Existing activations will not be changed.

#### Apply to all of the domain's activated accounts

If you wish to apply a policy to all devices already activated on a domain, select a domain and policy from the drop-down lists and then click this button. The policy will be applied to **all** activated accounts on the domain—even to those accounts that have had a different policy assigned to them on the Account Editor's BlackBerry Enterprise Server[351] screen.

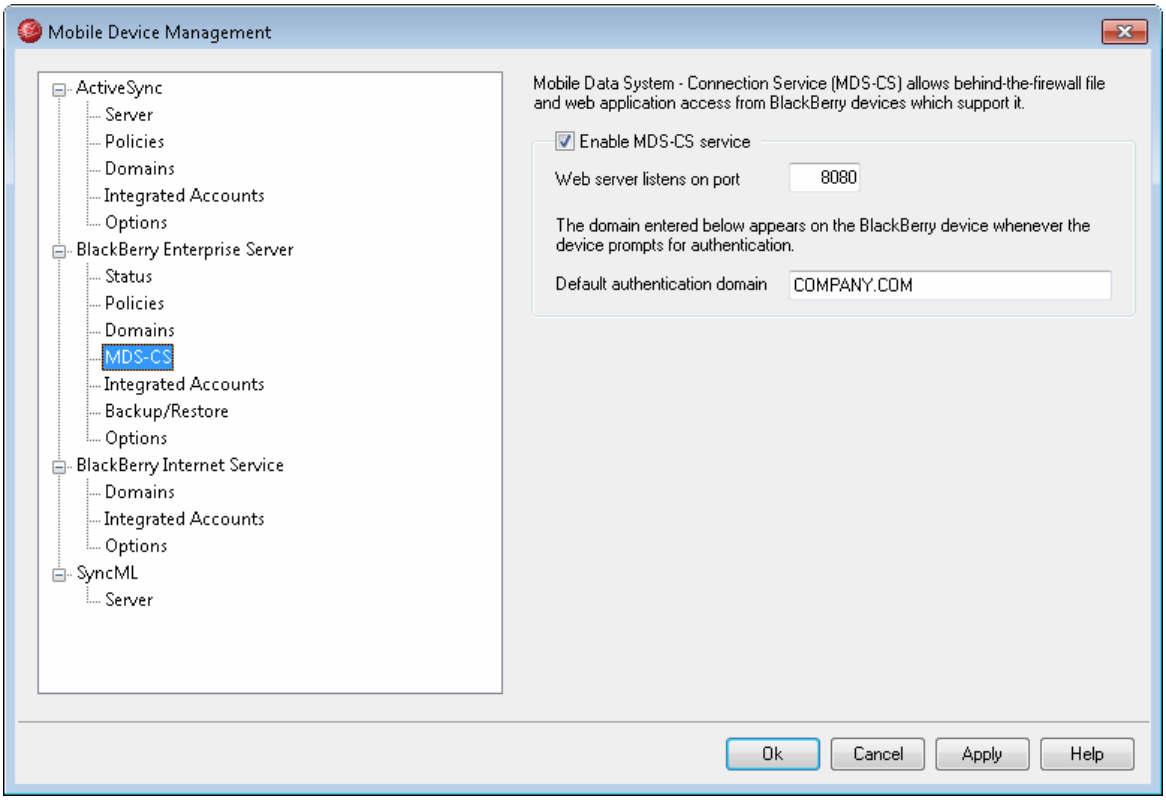
---

**See:**

**BlackBerry Enterprise Server**[162]
**Account Editor » BlackBerry Enterprise Server**[351]

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.2.4 MDS-CS




**BlackBerry® Mobile Data System Connection Service (MDS-CS)**

MDS-CS permits behind-the-firewall access to files and web applications from BlackBerry devices. It receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, and sends login requests so that users can view Internet and Intranet content on their BlackBerry devices. This will, for example, allow you to access your private Intranet without a VPN connection.

You can find more information about MDS-CS at BlackBerry.com, but please note that not all of the features and capabilities documented there are supported by MDaemon.

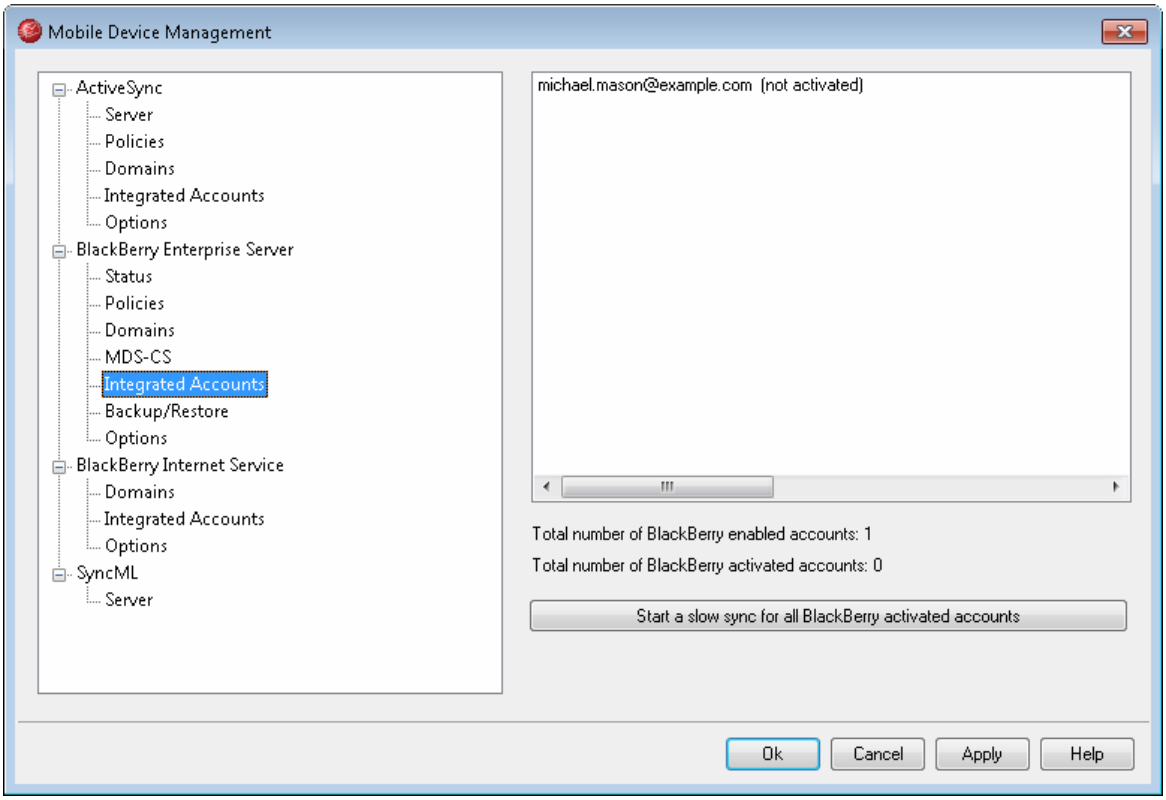
**Enable MDS-CS service**
Clear this check box if you do not wish to run the BlackBerry MDS Connection Service.

**Web server listens on port**
This is the port on which the web server will listen for connections from your BlackBerry devices.

**Default authentication domain**
This is the domain value that will appear on the BlackBerry device anytime the device prompts the user for authentication related to MDS-CS activities.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.2.5 Integrated Accounts




This screen lists all accounts that have been enabled for BlackBerry device synchronization, and their current state: activated or not activated. Activated accounts also display the activated device's PIN. Under the account list is a counter that tells you the number of accounts that are enabled for BlackBerry device synchronization and the number of accounts that are activated.

**Start a slow sync for all BlackBerry activated accounts**
Click this button to initiate a slow sync of all activated accounts. This resynchronizes all account data, ensuring that the data on the devices matches the data in MDaemon. Depending on the number of accounts and amount of data to be synchronized, this could take a long time to complete. Once started it will continue in the background until finished. You will be asked to confirm the decision to start a slow sync. There is an option located on the Account Editor's BlackBerry Enterprise Server 351 screen that can be used to initiate a slow sync for a specific account. See Options 179 for more BlackBerry Enterprise Server synchronization options.

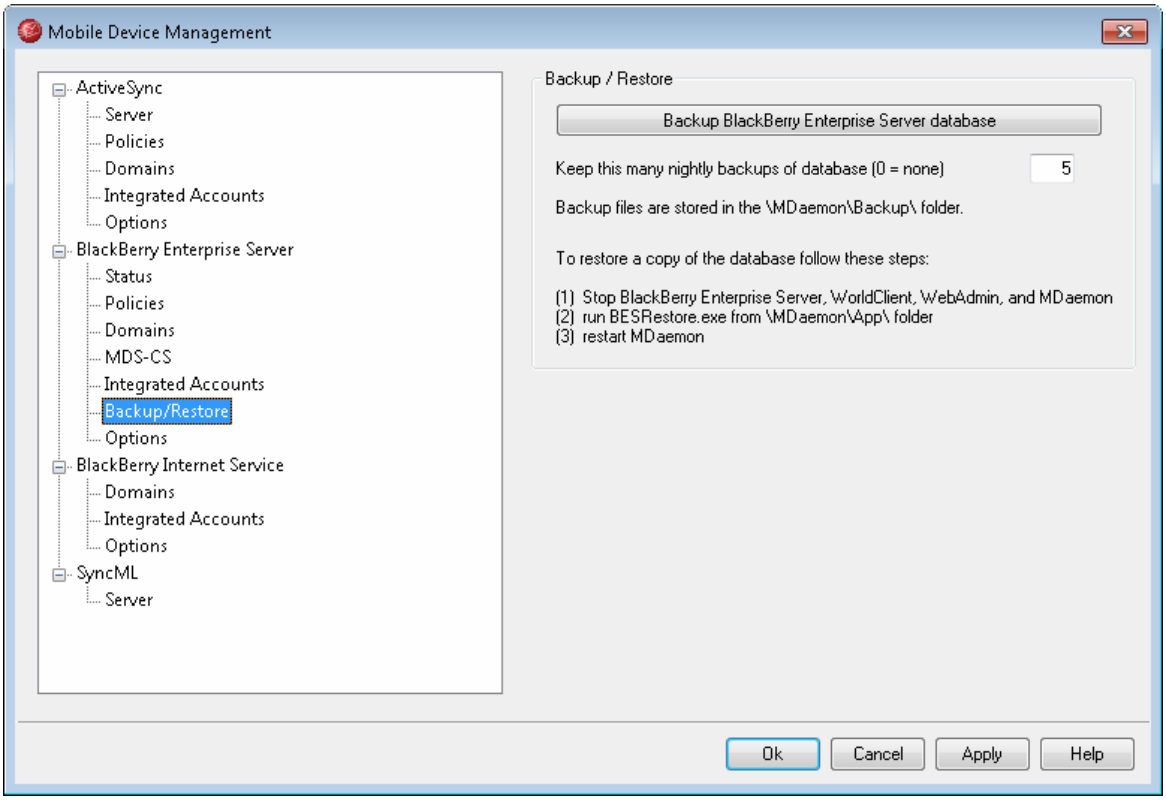
---

**See:**

**BlackBerry Enterprise Server** 162
**Account Editor » BlackBerry Enterprise Server** 351
**BlackBerry Enterprise Server » Options** 179

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.5.2.6 Backup/Restore




## Backing up the BlackBerry Enterprise Server database

Use the options on the Backup/Restore screen to backup your BlackBerry Enterprise Server database.

**Backup BlackBerry Enterprise Server database files**
Click this button if you wish to do an immediate, manual backup of your BlackBerry Enterprise Server database. The backup file is stored in the `\MDaemon\Backup\` folder. An entry about the backup's progress will appear on the System tab of MDaemon's Main Display 31.

**Keep this many nightly backups of BlackBerry Enterprise Server database files (0=none)**
Each night the BlackBerry Enterprise Server database is backed up and the backup files are stored in the `\MDaemon\Backup\` folder. This option determines the number of backup files that will be saved. When the limit is reached, the oldest file will be deleted when a new backup file is created. Use "0" in this option if you do not wish to do automatic nightly backups.

This value limits the number of backup files that will be saved, including manual backups initiated by clicking the *Backup BlackBerry Enterprise Server database files* button. If the value is set to "0" then no nightly backup will be performed, but you can still do manual backups, and there is no limit to

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the number of manual backup files that can be saved.

## Restoring the BlackBerry Enterprise Server database

To restore your BlackBerry Enterprise Server database from a backup file:

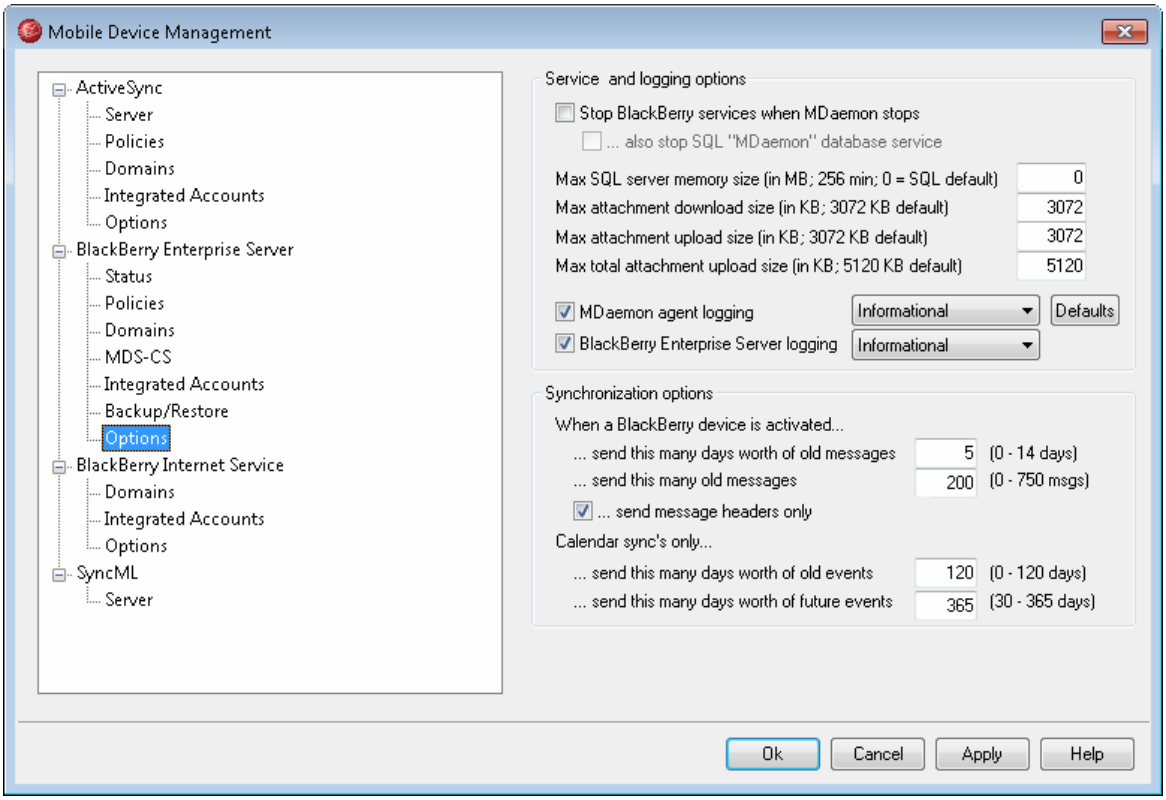
1. Stop the BlackBerry Enterprise Server, WorldClient, WebAdmin, and finally MDaemon.
2. Run the MDaemon BlackBerry Enterprise Server Database Restore Utility ( `BESRestore.exe`) in the `\MDaemon\App\` folder.
3. Click **Browse** and select the backup file.
4. Click **Open**.
5. Click **Restore Now**.
6. Restart MDaemon, WebAdmin, WorldClient, and the BlackBerry Enterprise Server.

**See:**

**BlackBerry Enterprise Server** 162
**Account Editor » BlackBerry Enterprise Server** 351

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.5.2.7 Options




With this screen you can set the BlackBerry Enterprise Server services to stop when MDaemon stops, configure logging options, and set several synchronization options for email and calendar data.

#### Service Options

**Stop BlackBerry services when MDaemon stops**
Check this box if you want the BlackBerry services 166 to stop whenever MDaemon stops.

**...also stop SQL "MDaemon" database service**
If you configure the BlackBerry services to stop when MDaemon stops, and you want the SQL "MDaemon" database service to stop also, then click this checkbox. Ordinarily the SQL "MDaemon" database service is left running, even if MDaemon or the BlackBerry services are stopped.

**Max SQL server memory size (in MB; 256 min; 0=SQL default)**
You can use this option to set a maximum memory size for the SQL server. This value is in MB and it must be set to at least "256". Use "0" in this option if you wish to use the SQL default setting.

**Max attachment download size (in KB; 3072 KB default)**
Use this option to specify the maximum size of attachments that can be downloaded to a BlackBerry device.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Max attachment upload size (in KB; 3072 KB default)**
This option specifies the maximum size of each separate attachment that can be uploaded in an email from a BlackBerry device.

**Max total attachment upload size (in KB; 5120 KB default)**
This is the maximum combined size of attachments that can be uploaded together in an email message from a BlackBerry device.

### Logging Options

There are two BlackBerry logging options: **MDaemon agent logging** and **BlackBerry Enterprise Server component logging**. You can enable/disable them separately and set the level of logging detail that will be maintained for each. There are four levels of logging detail to choose from: *Error*, *Warning*, *Informational*, and *Debug*. *Error* is the lowest level of logging and *Debug* is the highest, which should generally be used only when diagnosing a problem. *Informational* maintains a good level of detail and is the default setting for both options. Click **Defaults** to restore the logging levels to the default settings.

Whenever you change the logging level the BlackBerry Enterprise Server services will be restarted.

The BlackBerry log files use MDaemon's global Logging 103 settings for size and roll-over but are slightly different in format than other MDaemon logs. The logs are stored in the `\Logs\BES\` subfolder.

### Synchronization Options

**When a device is activated...**
These option are used to ensure that when a BlackBerry device is first activated, some of its old mail (mail sent or received prior to activation) will be synchronized with the device rather than only new mail. All mail processed for the account between the time it was enabled for BlackBerry device synchronization 351 and the device was activated will be synchronized with the device. If the number of messages or number of days worth of messages specified below have not been exceeded by the initial synch, then more mail will be synchronized according to the options.

**...send this many days worth of old messages to the BlackBerry**
Use this option to set the minimum number of days worth of old messages to send to the device when it is first activated. If it is set to 5, for example, then at least the last five days worth of messages will be sent.

This setting is also used during resynchronization (slow sync 176). Slow sync will only add messages missing from the database if they are more recent than the number of days specified here.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...send this many old messages to the BlackBerry**
Use this option to set the number of old messages to synchronize with the device when it is first activated. This option takes precedence over the "*...send this many days worth of old messages*" option above, and the initial synchronization after activation may exceed this number of messages if more than that are processed between the time the account is enabled for BlackBerry device synchronization and when the device is activated. This option is set to **200** by default.

**...send message headers only**
Use this option to send only the message headers to the device rather than the entire message when old messages are synchronized.

**Calendar syncs only...**
These options determine the number of calendar events that will be synchronized with activated BlackBerry devices. Whenever these values are changed, a slow sync 176 must be performed in order for any events that would be affected by the change to be added or deleted from the devices. A calendar slow sync occurs automatically every night at midnight.

**...send this many days worth of old events to the BlackBerry**
This is the number of days worth of past calendar events that will be synchronized with the BlackBerry device calendar. Recurring events older than this number of days will still appear on the device calendar if one of the event's occurrences lies within the designated limit.

**...send this many days worth of future events to the BlackBerry**
This is the number of days worth of future events that will be synchronized with the BlackBerry device.

If there are any existing calendar entries on the device before it is activated, you must either wipe the device or reset the calendar. Otherwise existing calendar data on the MDaemon server may not be sent to the device. If you choose to reset the calendar rather than wipe the device, the reset may be performed after activation. See **Resetting the Device Calendar** below for more information. Always backup your device data before erasing it or resetting the calendar.

## Resetting the Device Calendar

### Overview (article KB15139)

**Warning:** The following procedures will delete all calendar data on the BlackBerry smartphone and re-synchronize the calendar back to the BlackBerry smartphone.

**Note:** Back up the data prior to performing the procedure. For instructions, see

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

article KB12487.

Complete the steps for the version of BlackBerry Device Software installed on the BlackBerry smartphone.

**BlackBerry Device Software version 4.2**

On the BlackBerry smartphone, complete the following steps:

1. On the menu in the Calendar application, click **Options**.
2. Scroll to the bottom of the screen, and type **RSET**.

**Note:** For BlackBerry smartphones that support SureType® technology, use the multi-tap input method.

**BlackBerry Device Software version 4.3 to 5.0**

On the BlackBerry smartphone, complete the following steps:

1. On the menu in the Calendar application, click **Options**.
2. While the Options screen is displayed, type **RSET**.

**Note:** For BlackBerry smartphones that support SureType technology, use the multi-tap input method.

## Additional Information

### Wireless calendar synchronization process

#### Wireless calendar synchronization is turned on

If wireless synchronization of the calendar is turned **on**, the following message will appear:

*This will erase your <nameofcalendar> calendar, and reload it from your server. Continue?*

After the calendar data has been deleted, the following message will appear:

*The <nameofcalendar> calendar has been wiped. It will be repopulated from your server.*

The calendar will be repopulated with calendar data from the BlackBerry Enterprise Server.

#### Wireless calendar synchronization is turned off

If wireless synchronization of the calendar is turned **off**, the following message will appear:

*Wireless Calendar, for <nameofcalendar>, is not enabled. Wipe Calendar anyway?*

After the calendar data has been deleted, the following message will appear:

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*The <nameofcalendar> calendar has been wiped.*

The calendar must then be repopulated with calendar data using BlackBerry Desktop Manager through a wired synchronization.

**Re-population of calendar**

During re-population of the calendar, the following message may appear on the BlackBerry smartphone:

*Organizing Calendar*

The performance of the BlackBerry smartphone may be affected during the re-population of the calendar. The speed of re-population depends on the amount of data transmitted and the speed of the wireless network.

**See:**

**BlackBerry Enterprise Server** 162
**Account Editor » BlackBerry Enterprise Server** 351

### 4.5.3 BlackBerry Internet Service

MDaemon is equipped with direct support for the BlackBerry Internet Service (BIS). BlackBerry Internet Service users can integrate their MDaemon mail account with their BlackBerry smartphone, allowing for BlackBerry push mail as well as improved email handling when using a BlackBerry device with MDaemon. Any BlackBerry device set up to pull mail from MDaemon via IMAP or POP prior to MDaemon version 11.0 can now be set up for push mail instead. Further, messages that are composed on the device will be sent to your MDaemon for delivery rather than having the BlackBerry Internet Service servers deliver them. This allows emails composed on a BlackBerry device to comply with your server's security policies, content-filter rules, DKIM, archiving, and so on.

Since the BlackBerry Internet Service only collects mail from a user's Inbox, this can cause problems for people who use IMAP Filters 356 to sort their messages to specific folders automatically. To overcome this problem, the BlackBerry Inbox 353 screen of the Account Editor and the Folders page in WorldClient allow the administrators and users, respectively, to choose which folders' new messages will be delivered to the user's device. When the BlackBerry Internet Service connects to MDaemon to collect new messages from the user's Inbox, MDaemon will also push the new messages from the selected folders. All new messages from all the selected folders will be sent to the BlackBerry device's Inbox. This does not push the actual folders to the device, it pushes only the new messages that they contain.

Finally, an internal folder aliasing scheme allows each user's "Sent Items" and "Deleted Items" folders to appear as values that the BlackBerry Internet Service recognizes, no matter what those folders are actually called in the user's account. This helps ensure that sent and deleted messages are placed into the proper MDaemon folders.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

The BlackBerry Internet Service section of the BlackBerry dialog contains the following screens:

**Domains**185 — use this screen to enable BlackBerry Internet Service integration for whichever domains you choose. There are options for entering the Subscribe URL and the SMTP server to which the BlackBerry Internet Service should pass messages when they are composed on a BlackBerry device. There is a history text box on the bottom of the screen that lists your BlackBerry Internet Service subscribe/unsubscribe activity, and there are several SSL and STARTTLS related options.

**Integrated Accounts**187 — this screen lists the subscription numbers of all MDaemon accounts that are setup for BlackBerry Internet Service push mail and are thus integrated directly with MDaemon. Even if an account is not listed as an integrated account, a BlackBerry Internet Service server may still be able to collect mail on behalf of the BlackBerry device via POP3 or IMAP, but it will not have the advantage of being able to send messages through your MDaemon server.

**Options**189 — this screen has several global options governing MDaemon's BlackBerry integration features. For example, you can choose whether or not to allow MDaemon to push mail from non-Inbox folders, you can choose to apply Attachment Linking142 to integrated accounts, you can allow multiple devices to integrate with a single MDaemon account, and several other options.

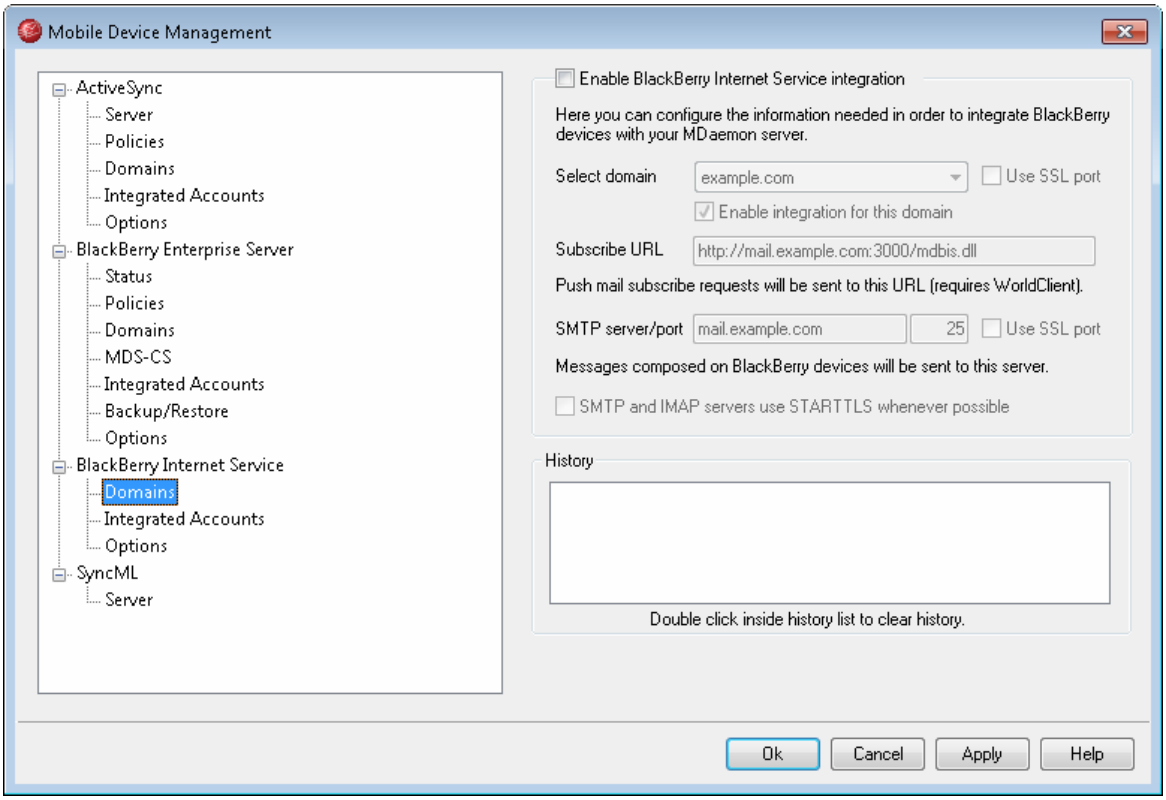
MDaemon requires all IMAP/POP sessions from BlackBerry Internet Service users to use a full email address when logging in to MDaemon. Thus when configuring their BlackBerry devices to collect mail they will need to use the full email address as the login parameter instead of just the mailbox portion of the address. This is necessary in order to avoid possible conflicts and to achieve proper account integration. This might mean that some of your existing users will have to delete and recreate the mail profile on their device, or at least change their login value to the full address.

**See:**

**BlackBerry Internet Service » Domains**185
**BlackBerry Internet Service » Integrated Accounts**187
**BlackBerry Internet Service » Options**189
**Account Editor » BlackBerry Internet Service**353

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 4.5.3.1 Domains




**Enable BlackBerry Internet Service (BIS) integration**

Check this box if you wish to enable MDaemon's BlackBerry Internet Service integration feature. You can then enable/disable it for individual domains by using the options below.

When BlackBerry Internet Service integration is disabled globally or for particular domains, any accounts already subscribed to the BlackBerry Internet Service will continue to operate as before. No future BlackBerry devices will be integrated, but any existing integrations are unaffected.

**Select domain**

Select the domain in the drop-down list that you wish to configure for BlackBerry Internet Service integration. Any changes you make to the remaining settings will apply only to that domain.

**Enable BlackBerry Internet Service integration for this domain**

Click this option to activate the BlackBerry Internet Service integration feature for the selected domain.

**Use SSL port**

If you have enabled SSL 310 in MDaemon, check this box if you want the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

BlackBerry Internet Service IMAP client to use the dedicated SSL port. The BlackBerry Internet Service IMAP client only supports SSL on the dedicated port.

**Subscribe URL**
This is the WorldClient URL to which the BlackBerry Internet Service will send subscribe and unsubscribe requests. When a user adds his MDaemon email account to his BlackBerry device, the BlackBerry Internet Service will send a subscribe request to this URL within approximately twenty minutes. MDaemon will then add the account to the Integrated Accounts 187 screen. Subscription requests are managed by WorldClient, therefore WorldClient must be active.

When using IIS rather than WorldClient's native web server, you must add `MDbis.dll` (located in `MDaemon\Worldclient\HTML\`) to IIS in order for incoming SUBSCRIBE commands to be processed properly.

**SMTP Server/port**
This is the SMTP server and port to which all email composed on the integrated account's device will be sent for delivery.

**Use SSL port**
If you have enabled SSL 310 in MDaemon, check this box if you want the BlackBerry Internet Service SMTP client to use the dedicated SSL port.

The BlackBerry Internet Service SMTP client does not support SSL with self-signed certificates. Therefore if you wish to use SSL then you must use a commercial, third-party certificate.

**SMTP and IMAP servers use STARTTLS whenever possible**
When MDaemon's STARTTLS 310 feature is enabled, check this box if you want the SMTP and IMAP servers to use STARTTLS whenever possible.

The BlackBerry Internet Service does not support STARTTLS with self-signed certificates. Therefore if you wish to use STARTTLS then you must use a commercial, third-party certificate.

## History

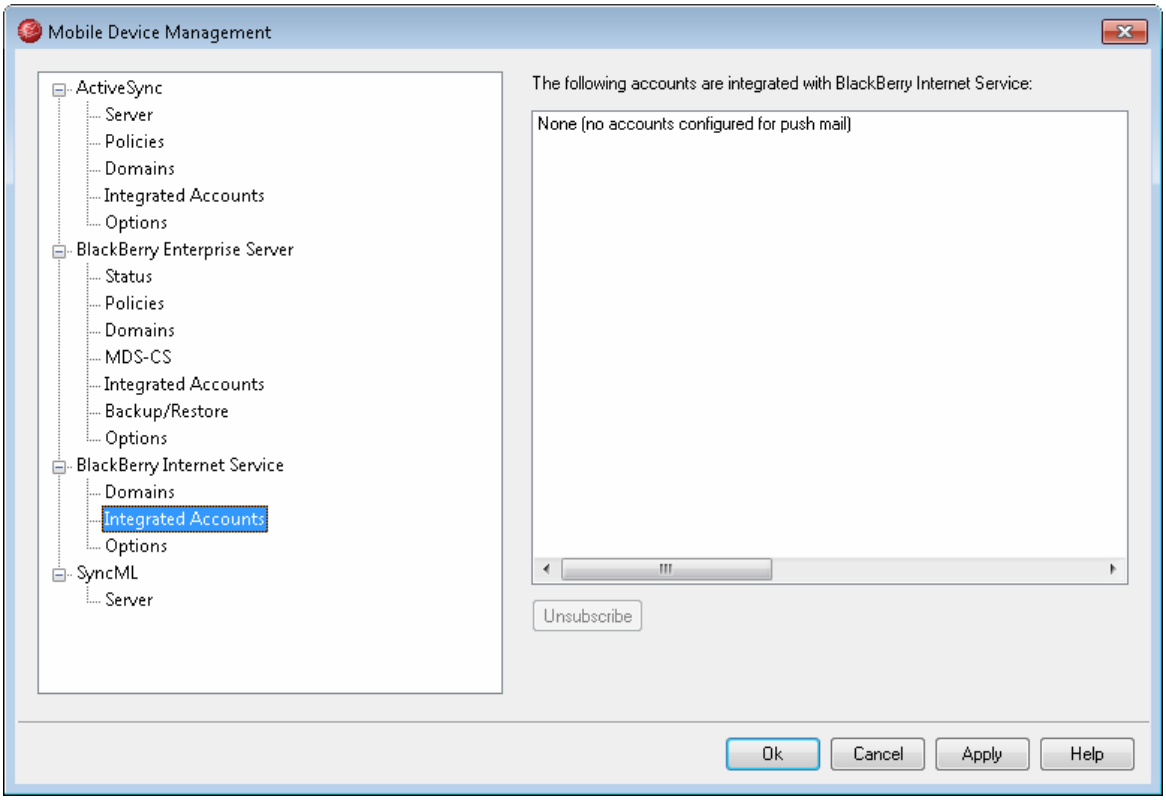
This box lists the BlackBerry Internet Service subscribe/unsubscribe history for your accounts. Each entry lists whether it was a subscribe or unsubscribe action, the email address, and the date and time of the activity.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

[BlackBerry Internet Service](#) 183
[BlackBerry Internet Service » Integrated Accounts](#) 187
[BlackBerry Internet Service » Options](#) 189
[Account Editor » BlackBerry Internet Service](#) 353

### 4.5.3.2 Integrated Accounts




## Configuring Accounts to Push Mail to a BlackBerry Smartphone

The Integrated Accounts screen lists all of your MDaemon accounts that are configured to push mail to a BlackBerry smartphone. To setup a new account for push mail:

1. Enable the BlackBerry Internet Service integration options for the server and domain on the Domains 185 screen, and make sure that the *Subscribe URL* and *SMTP server* value are pointing to WorldClient and your MDaemon server, respectively.
2. If the BlackBerry smartphone is already collecting mail from the user's MDaemon account, because the account was added to the device prior to activating MDaemon's BlackBerry Internet Service features, then delete that

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

email account from the device. In the next step you will need to recreate the account on the device so that you can trigger push mail setup within the BlackBerry Internet Service.

3. Add the MDaemon email account to the user's BlackBerry smartphone, using the **full email address** and password as its login credentials. For detailed instructions on how to add an email account to a BlackBerry smartphone, see the device's online help or documentaion. You must only add the account in this step, not edit it. After creating the account, do not edit its signature, name settings, advanced options, or the like. You can make changes to the account later, in step 6.
4. Shortly after the account is added to the device, the *Subscribe URL* associated with the user's domain will receive a SUBSCRIBE request from the BlackBerry Internet Service service. This incoming request will be processed by WorldClient and the subscribed account will appear in the Integrated Accounts list. The SUBSCRIBE request usually takes about 5 minutes to arrive, but can take up to 20.
5. Almost immediately after adding the account to the device it should receive an "*Email activation information*" email. Then, once the SUBSCRIBE request is properly received and processed, the BlackBerry device will receive a second email: "*Email activation information (push mail)*." Once that second email is received you know that the account has been successfully configured for push mail in MDaemon.
6. Make any desired changes to the email account on the device. You can add a signature, edit the name, adjust the advanced settings, and so on.

While waiting for the SUBSCRIBE request from the BlackBerry Internet Service to arrive, any changes to the email account on the device (such as signature text, advanced setup options, etc) will invalidate the request and you will not receive it. Therefore you must make no changes to the account on the device until the SUBSCRIBE request arrives. Otherwise you will need to delete the account and recreate it in order to restart the SUBSCRIBE process.

This level of integration is not possible using POP. Any of your BlackBerry users currently using POP to collect mail will need to delete their email profile and recreate it using IMAP (not POP) which may require accessing advanced setup options on the BlackBerry. Consequently, MDaemon's IMAP server must be running for this feature to work.

## Unsubscribing an Integrated Account

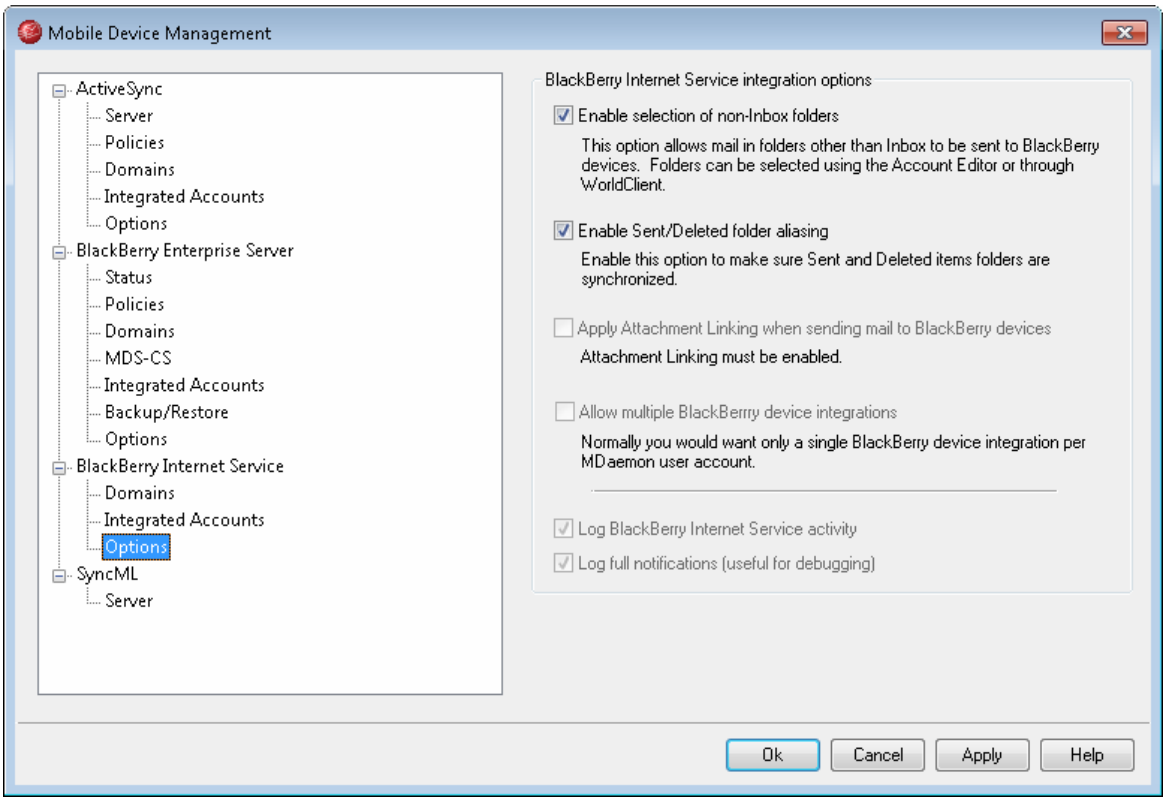
Unsubscribing from push mail can be done by deleting the email profile using the BlackBerry device itself. The BlackBerry Internet Service will then send MDaemon an UNSUBSCRIBE request and the account will be unlinked. The UNSUBSCRIBE request may take some time to arrive and this poses no operational issues.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**BlackBerry Internet Service** 183
**BlackBerry Internet Service » Domains** 185
**BlackBerry Internet Service » Options** 189
**Account Editor » BlackBerry Internet Service** 353

### 4.5.3.3 Options




#### BlackBerry Internet Service Integration Options

**Enable selection of non-Inbox folders**
By default in MDaemon, messages placed in non-Inbox IMAP folders can be pushed to a BlackBerry smartphone's Inbox. This is managed through the BlackBerry Inbox 353 screen of the Account Editor and the Folders page in WorldClient. These screens allow the administrators and users, respectively, to choose which folders' new messages will be delivered to the user's device. If you do not wish to allow users with a BlackBerry device to collect mail from any of their IMAP folders other than the Inbox, then disable this option. However, we recommend that you leave this option enabled, because if you disable it then those who use IMAP Filters 356 to sort their messages into specific folders will not be able to get those filtered messages on their device.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

This feature operates independently from the account integration options on the Domains[185] and Integrated Accounts[187] screens. Even if you disable BlackBerry Internet Service integration in MDaemon, a user can still create an email account on his BlackBerry device to collect his mail from MDaemon, just as he can collect it using any other traditional email client or smartphone. This feature simply makes it possible for BlackBerry smartphone users to collect messages from the folders that they are using IMAP filters to manage.

**Enable Sent/Deleted folder aliasing for BlackBerry users**
By default an internal folder aliasing scheme allows each user's "Sent Items" and "Deleted Items" folders to appear as values that the BlackBerry Internet Service recognizes, no matter what those folders are actually called in the user's account. This doesn't alter any folder names in any way. It is entirely an internal aliasing function to help ensure that sent and deleted messages are placed into the proper MDaemon folders. As with the above option, this option operates independently from the account integration options. It can be used even if the *Enable BlackBerry Internet Service integration* option is disabled on the Domains screen. If you do not wish to alias these folders for BlackBerry users, disable this option.

Users can designate the folders they wish to use as their Sent Items and Deleted Items folders from the Folders page in WorldClient.

**Apply Attachment Linking to BlackBerry integrated accounts**
Check this box if you wish to apply the Attachment Linking[142] feature to all messages sent to BlackBerry Integrated Accounts[187]. The *Enable attachment linking* feature on the Attachment Linking dialog must be enabled for this to work.

**Allow multiple BlackBerrys to integrate with same MDaemon account**
Enable this option if you wish to allow multiple BlackBerry devices to integrate with the same MDaemon account. This means, for example, that someone with two BlackBerry smartphones could set up both devices to get push mail from the user's single account.

**Log BlackBerry Internet Service IMAP activity (activity will be shown on the BIS log tab)**
Check this box if you wish to log the BlackBerry Internet Service IMAP activity. It will be copied to the log files and appear on the BIS tab of the main GUI.

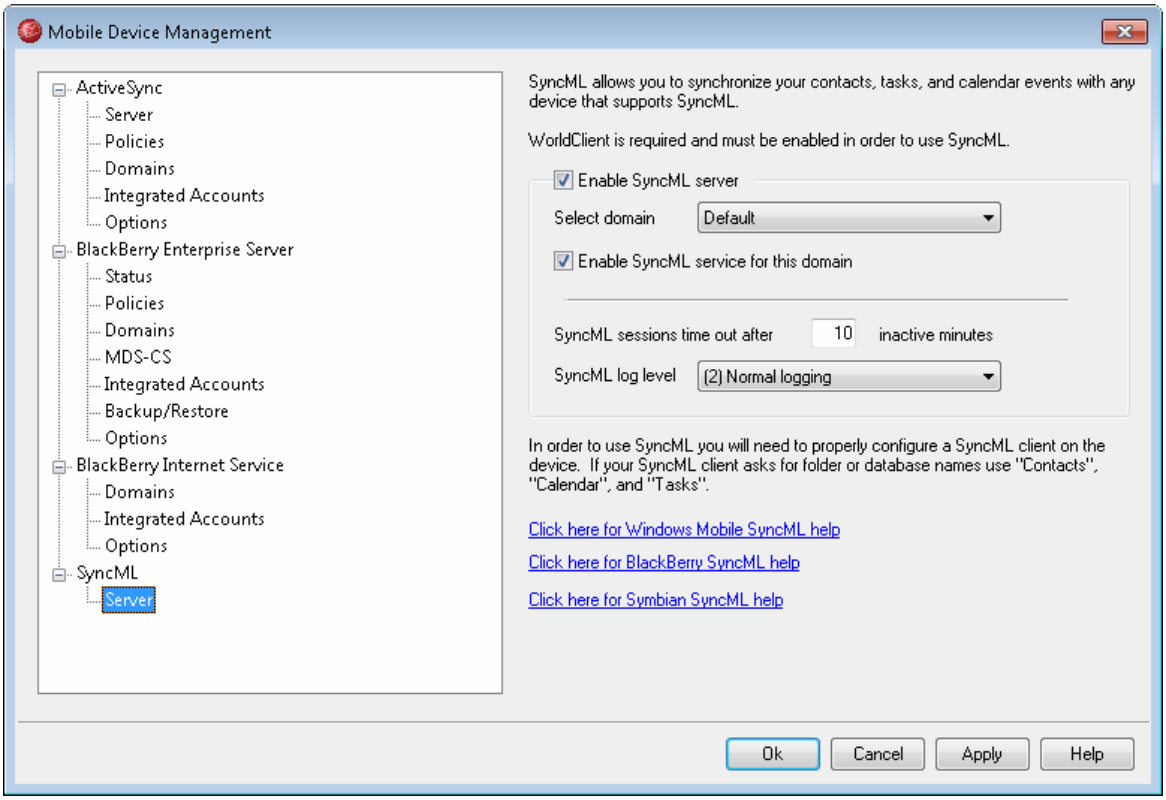
**Log full notifications from BlackBerry Internet Service servers (useful for debugging)**
Check this box if you wish to log all activity from BlackBerry Internet Service servers. This option can be useful for debugging, to help you diagnose BlackBerry Internet Service related problems.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**See:**

**BlackBerry Internet Service** 183
**BlackBerry Internet Service » Domains** 185
**BlackBerry Internet Service » Integrated Accounts** 187
**Account Editor » BlackBerry Internet Service** 353

### 4.5.4 SyncML




WorldClient includes a SyncML server that can be used to synchronize your Contacts, Tasks, and Calendar events with any SyncML capable mobile devices. If your BlackBerry smartphone or other device doesn't have built-in SyncML support then you must install a third-party synchronization client on it. Some example clients are: Funambol Sync Client, Synthesis, and SyncJE. There are also sync clients available for synchronizing your calendar with an email client such as Microsoft Outlook. The Funambol Sync Client, for example, is available for Outlook, BlackBerry, Windows Mobile, and other types of applications and devices. Several clients are available free of charge.

For more information on SyncML and the SyncML specification, visit the Open Mobile Alliance (OMA).

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**SyncML**

**Select domain**
Use this drop-down list box to choose the domain you wish to configure. After selecting the domain, check or uncheck the "*Enable SyncML server*" box and then click Apply or OK to save the setting. Choose "Default" from the drop-down list to designate the default setting. The default setting will be applied to all new domains and all existing domain for which you have not specifically defined a SyncML setting.

**Enable SyncML server**
Enable or disable this option to designate whether or not the SyncML server will be accessible by the domain selected in the *Select domain* option above.

**SyncML sessions time out after XX inactive minutes**
This is the length of time a SyncML session will be permitted to remain inactive before it will time out and be closed. This is a global setting—it applies to all SyncML sessions regardless of the domain.

**SyncML log level**
Use this drop-down list to designate the degree to which SyncML activities will be logged. There are six possible levels of logging: 1-Debug logging, 2-Normal logging, 3-Warnings and errors only, 4-Errors only, 5-Critical errors only, and 6-No logging. This is a global setting—it cannot be applied to specific domains.

### 4.5.4.1 Configuring Your SyncML Clients

In order to access WorldClient's SyncML server, your SyncML clients must be configured to connect to:

```
http://<WorldClient Server><:port>/MDSyncML.dll
```

Examples:

```
http://mail.example.com:3000/MDSyncML.dll
http://www.example.com/MDSyncML.dll
```

If your SyncML client asks for folder names, use `Contacts`, `Calendar`, and `Tasks`. Those names always expand to the user's default WorldClient folders of the corresponding type.

The SyncML server supports any of the following formats for the folder paths:

```
contacts
/contacts
./contacts
contacts/phone (assuming a phone sub-folder exists)
contacts.imap\phone.imap
```

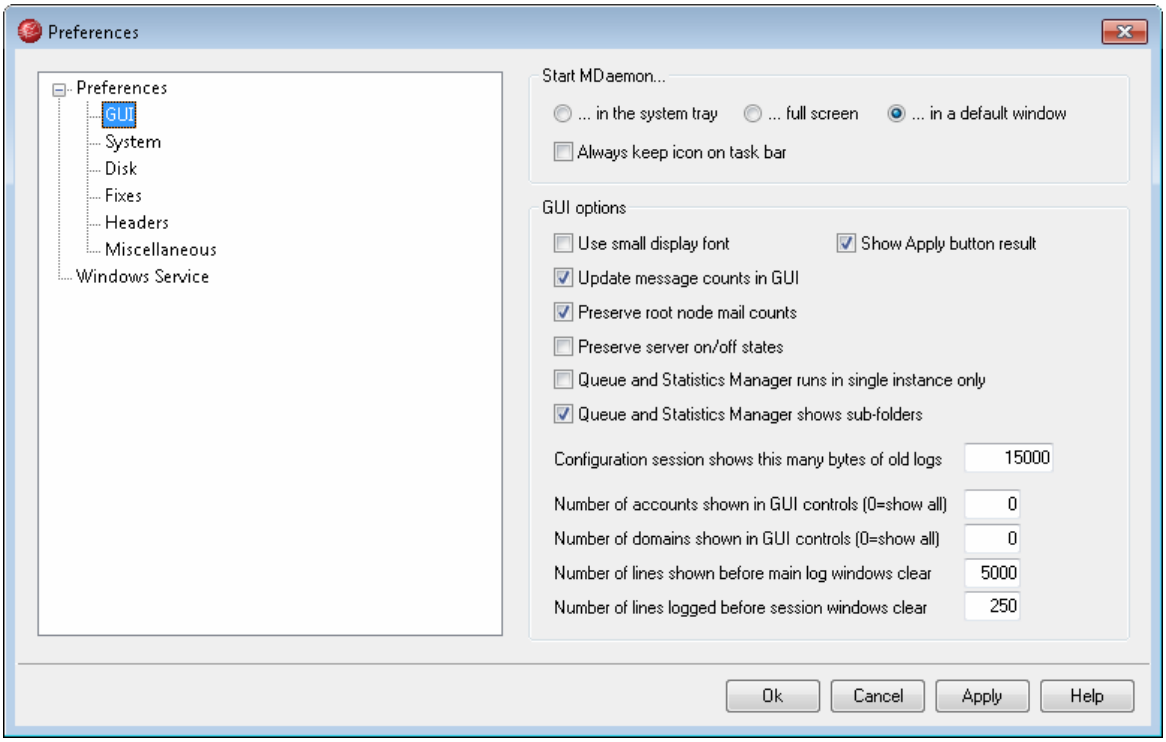
Before attempting to synchronize using SyncML, a user must log in to WorldClient one time.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# 4.6 Preferences

## 4.6.1 Preferences

### 4.6.1.1 GUI




**Start MDaemon...**

**...in the system tray**
Choose this option if you do not wish to display MDaemon's interface at startup. The MDaemon icon will still appear in the system tray.

**...full screen**
Choose this option if you want MDaemon's interface to be maximized at startup.

**...in a default window**
Choose this option if you want MDaemon's interface to appear in a default window at startup.

**Always keep icon on task bar**
When this option is enabled, MDaemon will start minimized to the taskbar, and it will appear on both the taskbar and in the system tray when minimized. Clear this checkbox if you do not want MDaemon to appear on the Windows taskbar when minimized; only the tray icon will be visible.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## GUI Options

**Use small display font in log windows**
Enables the small display font in the Event Tracking and Session windows.

**Show Apply button result**
By default, whenever you click the Apply button on a dialog a message box will open confirming that the changes you made to the dialog's settings have been saved. Uncheck this box if you wish to apply the changes without displaying the message.

**Continually update GUI with latest message counts**
This option governs whether MDaemon will check the disk to count waiting messages in the mail queues.

**Preserve root node mail counters across reboots**
Enable this option if you wish to save the root node counters across server reboots. The root node counters are listed in the "Statistics" section of the Stats pane on MDaemon's main GUI.

**Preserve server on/off state across reboot**
If this control is enabled, MDaemon will ensure that the state of its servers (enabled or disabled) remains the same after a reboot.

**Queue and Statistics manager runs in a single instance only**
Click this checkbox if you do not want more than one copy of MDaemon's Queue and Statistics manager 491 to be able to run at once. Attempting to launch the manager when it is already running will simply cause the currently running instance to become the active window.

**Queue and Statistics manager shows subfolders**
Click this checkbox if you want the Queue and Statistics manager 491 to display subfolders contained in the various queues and user mail folders.

**Number of accounts shown in GUI controls (0=show all)**
This is the maximum number of accounts that will be shown in the drop-down list boxes on various dialogs. Further, when the value in this option is set lower than the number of accounts that currently exist, the "Edit Account" and "Delete Account" options will no longer appear on the Accounts menu; you will only be able to edit and delete accounts by using the Account Manager 340. You must restart MDaemon before any changes to this option will take effect. The default setting is "0", which causes all accounts to be shown.

**Number of domains shown in GUI controls (0=show all)**
This is the maximum number of domains that will be displayed on the main GUI, regardless of how many domains actually exist. After changing this value you must restart MDaemon before the changes will be visible. The default setting is "0", which causes all domains to be shown.

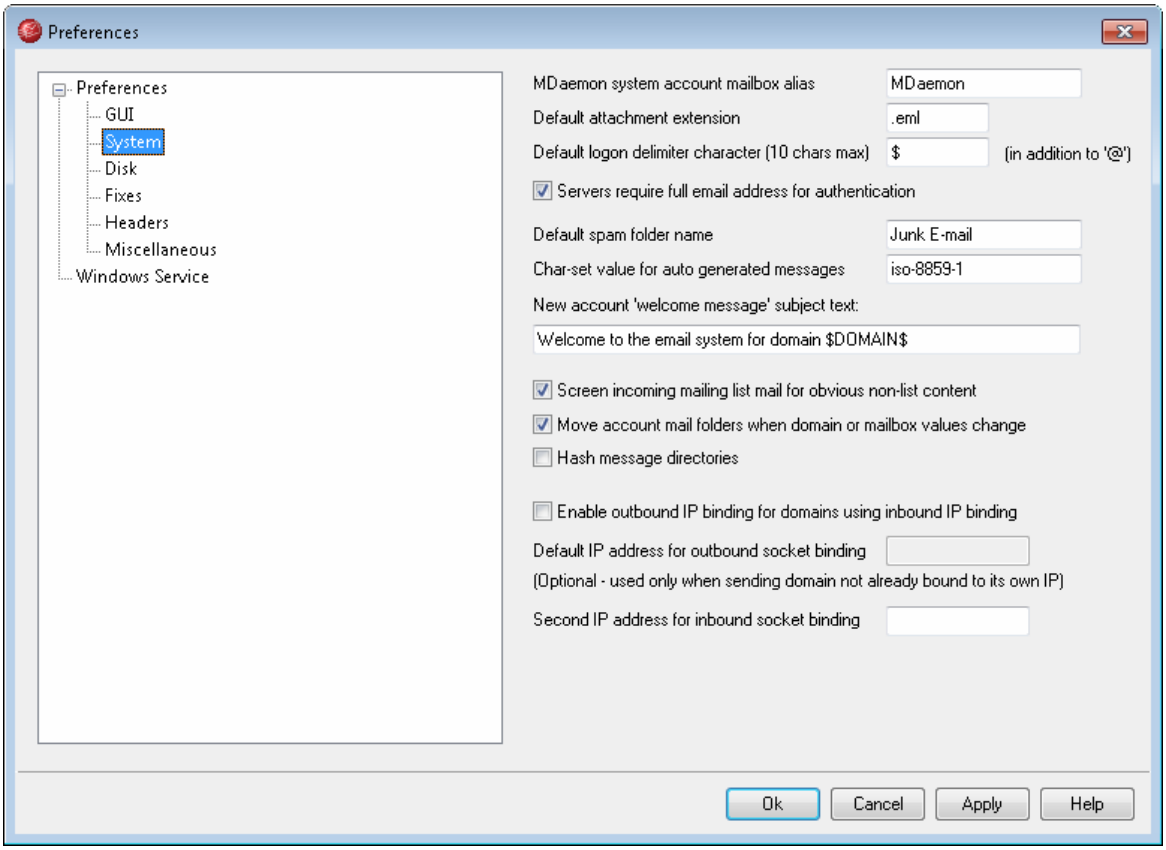
**Number of lines shown before main log windows clear**
This is the maximum number of lines that will be displayed in the logging windows of

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the main display. When this number of lines is reached the window will be cleared. This has no affect on the log file; only the display will be cleared.

**Number of lines logged before session windows clear**
This is the maximum number of lines that will appear in each Session Window 36 before it is cleared. This has no affect on the log file.

### 4.6.1.2 System




**MDaemon system account mailbox alias [address]**
This is the email address from which system generated messages will come. Subscription confirmations, delivery status notification (DSN) messages, various other notification messages, and the like are all system messages.

**Default attachment extension**
System generated messages will be created using this extension. This will also be the extension assigned to attachments included with system generated messages. For example, if MDaemon generates a warning message to the postmaster about a specific message it will attach that message with this value as the file extension.

**Default logon delimiter character (10 characters max)**
When using an email address as the account logon parameter, this character or

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

string of characters can be used as an alternative to "@". This may be necessary for some users that have email clients which do not support "@" in the logon field. For example, if you used "$" in this field then users could login using "user1@example.com" or "user1$example.com".

**Servers require full email address for authentication**
MDaemon's POP and IMAP servers require you to use your full email address by default when logging in to MDaemon. If you wish to allow mailbox only logins (e.g. "user1" instead of "user1@example.com") then you can disable this option, but it is not recommended as mailbox only logins are ambiguous when MDaemon is serving multiple domains.

**Default spam folder name**
Use this text box to specify the default name for the Spam folder that MDaemon can create automatically for your users. The default name is "Junk E-mail" to match the default value of various other widely distributed products.

**Char-set value for auto-generated messages**
Specify the character set that you wish to be used for auto-generated messages. The default setting is iso-8859-1.

**New account "welcome message" subject text:**
MDaemon typically sends a "welcome message" to new accounts. The text specified here will appear as the message's "Subject" header. The welcome message is constructed from the `NEWUSERHELP.DAT` file contained in the `…\MDaemon\app\` folder, and this subject header may contain any macros permitted in auto response scripts[393].

**Screen incoming mailing list mail for obvious non-list content**
Check this box if you wish MDaemon to reject messages addressed to a mailing list when it determines that they should have been addressed to the system account instead. For example, a user may join or leave a list by placing the Subscribe or Unsubscribe command at the beginning of an email message and sending that message to the system address (e.g. "mdaemon@example.com"). Oftentimes users erroneously try to send those sorts of messages to the list itself. This option will prevent those messages from being posted to the list.

**Move account mail folders when domain or mailbox values change**
If this checkbox is enabled, when you change a domain name or mailbox the mail folders for the affected accounts will be moved to the new location. Otherwise, MDaemon will continue to use the old mail folder names.

**Hash message directories**
Click this check box if you wish to enable directory hashing — MDaemon will hash certain directories by making up to 65 sub-directories. Hashing can increase performance for certain hi-volume sites but may degrade performance slightly for typical MDaemon sites. This option is disabled by default.

**Enable outbound IP binding for domains using inbound IP binding**
Click this option to cause domains that are using the *Restrict connections to this IP*

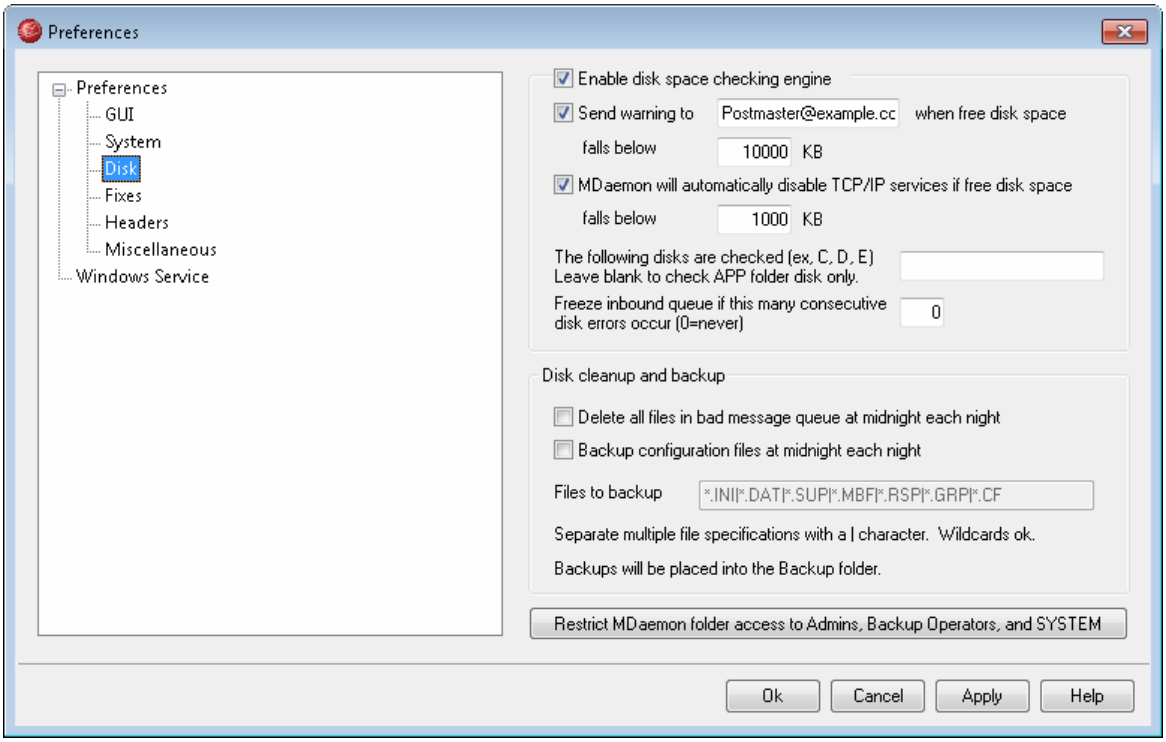
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

option to also restrict outbound sockets. The IP address that will be used is the same one that is associated with the handling of inbound mail, unless a different one is specified below.

**Default IP address for outbound socket binding**
This is the IP address that will be used for outbound socket binding. The setting is optional and only needed when the sending domain is not already restricted to its own IP addresses.

**Second IP address for inbound socket binding**
If you want the Default Domain's inbound sockets to be bound to an additional IP address then include it here.

### 4.6.1.3 Disk




**Enable disk space checking engine**
Activate this checkbox if you want MDaemon to monitor the amount of disk space that is available on the drive where the `MDaemon.exe` is located.

**Send warning to [user or address] when free disk space falls below [xx] KB**
By using this option you can configure MDaemon to send a notification message to the user or address of your choice when disk space drops below a certain level.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**MDaemon will automatically disable TCP/IP services if free disk space falls below [xx] KB**
Enable this feature if you want MDaemon to disable TCP/IP Services if free disk space drops to a certain level.

**The following disks are checked (ex: C, D, E)**
Use this option if you wish to monitor the available disk space on multiple disks, specifying the drive letter for each one. If you leave it blank then only the disk that contains MDaemon's `\app\` folder will be checked.

**Freeze inbound queue if this many consecutive disk errors occur (0=never)**
If this number of disk errors occurs when processing the inbound queue, MDaemon will stop processing the queue until you resolve the situation. An email is placed in the postmaster's mailbox when this shut down occurs.

### Disk cleanup and backup

**Delete all files in bad message queue at midnight each night**
Click this checkbox if you want MDaemon to delete all files from the bad message queue each night at midnight. This can help to conserve disk space.

**Backup configuration files at midnight each night**
Click this checkbox if you want to archive all MDaemon configuration files at midnight each night to the Backups directory.

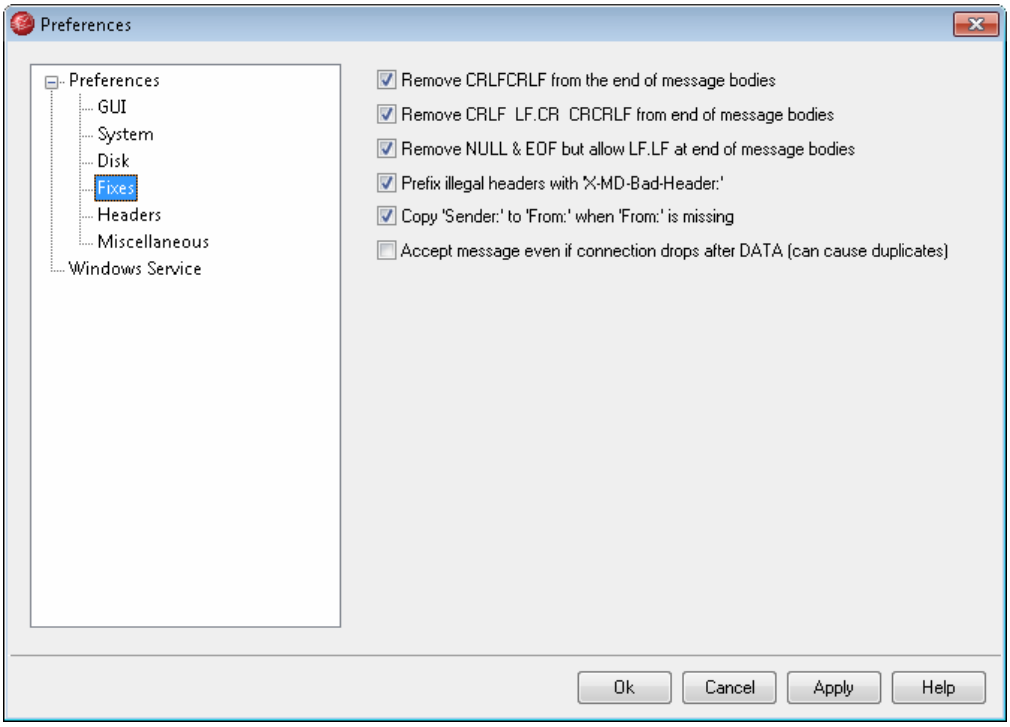
**Files to backup**
Use this text box to specify exactly which files and file extensions to back up. Wildcards are permitted and each filename or extension must be separated be the "|" character.

### Restrict MDaemon folder access to Admins, Backup Operators, and SYSTEM

Click this button to restrict access to the `\MDaemon\` root folder and its subfolders to the following Windows accounts/groups: Administrators, Backup Operators, and SYSTEM.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 4.6.1.4 Fixes




**Remove CRLFCRLF from the end of message bodies**
Certain mail clients have problems displaying messages that end with consecutive Carriage Return Line Feeds (i.e. CRLFCRLF). When this box is checked, MDaemon will strip consecutive `CRLFCRLF` sequences from the end of the message body. This option is enabled by default.

**Remove CRLF LF.CR CRCRLF from the end of message bodies**
By default, MDaemon will remove this sequence from the end of messages, as it can cause problems for some mail clients. Uncheck this box if you do not wish to remove this sequence from messages.

**Remove NULL & EOF but allow LF.LF at the end of message bodies**
When this box is checked MDaemon will remove `Null` and EOF characters from the end of message bodies, but it will allow messages ending in `LF.LF`, as well as messages ending with the normal `CRLF.CRLF` sequence that signifies the end of a message. This option is enabled by default.

**Prefix illegal headers with "X-MD-Bad-Header:"**
When this option is enabled and MDaemon encounters a bad message header, it will prefix the bad header with "`X-MD-Bad-Header:`" This option is enabled by default.

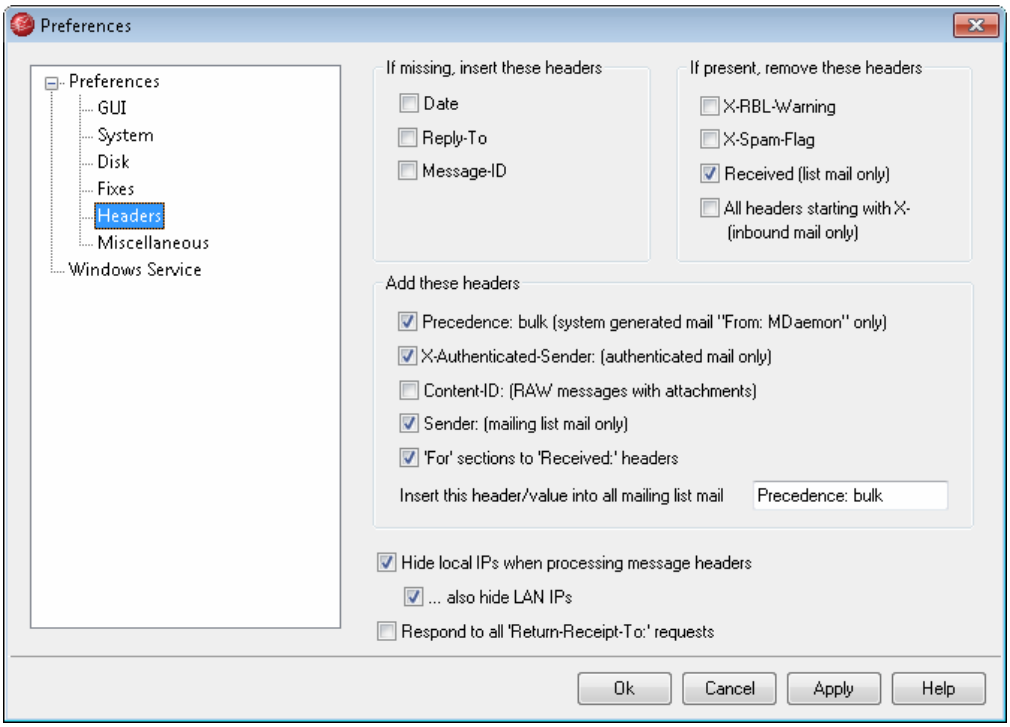
**Copy 'Sender:' to 'From:' when 'From:' is missing**
Some mail clients fail to create a `FROM:` header when you compose a message. Instead, the `FROM:` header's information is placed in the `Sender:` header. This can cause problems for some mail servers as well as the recipient of your message. To help prevent these problems, MDaemon will create the missing `FROM:` header by

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

using the contents of the `Sender:` header when this box is checked. This option is enabled by default.

**Accept message even if connection drops after DATA (can cause duplicates)**
When this option is enabled, MDaemon will accept and deliver a message even if there's a connection abort during or immediately after the `DATA` command during the SMTP process. This should not be used under normal circumstances as it can lead to duplicate messages.

### 4.6.1.5 Headers




**If missing, insert these headers**

**Date**
When a message is encountered that doesn't have a "`Date:`" header, MDaemon will create one and add it to the message file if this option is enabled. It will be the date on which MDaemon first receives the message, not when it was created by the sender. There are some mail clients that do not create this header, and since some mail servers refuse to honor such messages, this feature will enable them to be delivered.

**Reply-To**
When this option is enabled and a message is encountered that doesn't have a "`Reply-To`" header, MDaemon will create and add one to the message file using the address found in the "`From`" header. If a "`Reply-To`" header is present but **empty**, MDaemon will create the header like this: `Reply-To: ""`. This fixes problems for some

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

mail clients.

**Message-ID**
When a message is encountered that doesn't have a "Message-ID" header, MDaemon will create one and insert it into the message.

### If present, remove these headers

**X-RBL-Warning**
Click this checkbox if you wish to strip out all "X-RBL-Warning:" headers found in messages. This option is disabled by default.

**X-Spam-Flag**
Enable this option if you wish to strip old "X-Spam-Flag:" headers from messages.

**Received (list mail only)**
Check this box if you wish to strip all existing "Received:" headers from mailing list messages.

**All headers starting with X- (inbound mail only)**
MDaemon and other mail servers use many server specific headers called X-Type headers in order to route mail and perform various other functions. When this option is enabled, MDaemon will strip out these headers from inbound messages. **Note:** this option does not remove X-RBL-Warning headers.

### Add these headers

**Precedence: bulk (system generated mail 'From: MDaemon' only)**
When this box is checked all system generated messages from MDaemon (welcome messages, warnings, "could not deliver" messages, and so on) will have a "Precedence: bulk" header inserted.

**X-Authenticated-Sender: (authenticated mail only)**
By default MDaemon will add the "X-Authenticated-Sender:" header to messages that arrive on an authenticated session using the AUTH command. Uncheck this box if you do not wish to add this header.

**Content-ID: (RAW messages with attachments)**
Check this box if you wish to add unique MIME Content-ID headers to messages that MDaemon creates from a RAW file that contains attachments.

**Sender: (mailing list mail only)**
Enable this option if you wish to insert the Sender header into mailing list messages. **Note:** because the Sender header is required when DomainKeys signing list messages, this option will have no effect when you have configured MDaemon to DomainKeys sign them — all list mail will have a Sender header.

**'For' sections to 'Received:' headers**
Click this switch if you want "For [SMTP Recipient]" sections to be added to the message's "Received:" header added by MDaemon.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Insert this header/value into all mailing list mail [header]**
If you wish to add a static header/value combination (such as "Precedence: bulk") to all list messages, then specify that text here.

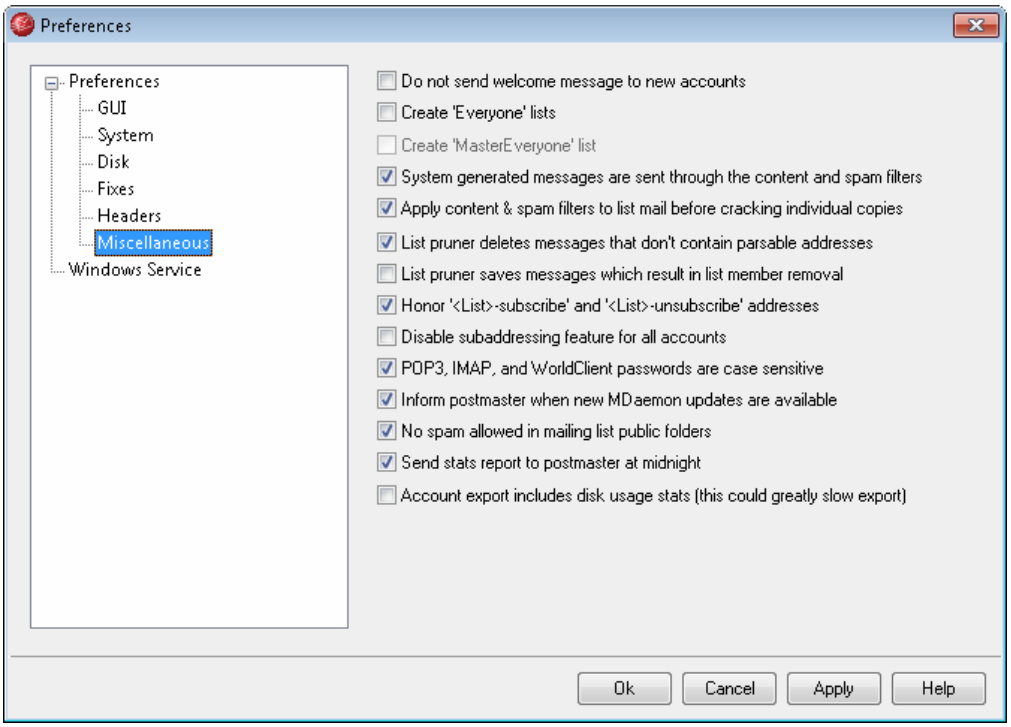
—

**Hide local IPs when processing message headers**
Click this option to prevent MDaemon from placing local IP addresses into message headers when it processes mail.

**...also hide LAN IPs**
If MDaemon is configured to hide local IP addresses, click this check box if you also wish to hide the IP addresses listed on the LAN IPs screen 336.

**Respond to all 'Return-Receipt-To:' requests**
Click this check box if you wish to honor requests for delivery confirmation from incoming messages and automatically send a confirmation message to the sender. This option is disabled by default.

### 4.6.1.6 Miscellaneous




**Do not send welcome message to new accounts**
By default, MDaemon will generate a Welcome message based upon the NEWUSERHELP.DAT file and distribute it to new users when their account is created. Enable this control if you want to prevent the message from being generated.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Create "Everyone" lists**
Check this box if you wish MDaemon to create and maintain "Everyone" mailing lists for your domains (e.g. "everyone@example.com"). Maintaining mailing lists of every user on every MDaemon domain could be a potential waste of resources if the lists are never used, or if they are for very large numbers of users. This option is disabled by default.

**Create "MasterEveryone" list**
Enable this option if you want there to be a "MasterEveryone" mailing list. Everyone on all of your domain-specific "everyone" lists will be included on this list. This option is disabled by default.

**System generated messages are sent through the Content Filter**
By default, system generated messages are processed through the Content Filter. Clear this checkbox if you want them to be excluded from content filtering.

**Apply content & spam filters to list mail before cracking individual copies**
When the *MDaemon will crack list mail* option is chosen on the Routing screen of the mailing list editor, enabling this control will cause the content filter rules and spam filter to be applied to list messages before they are cracked and distributed to list members.

**List pruner deletes messages that don't contain parsable addresses**
When you have configured MDaemon to scan messages that are returned to a Mailing List in an attempt to delete list members that cannot be reached, this control will cause those messages to be deleted that do not contain a parsable address. For more information, see the *Automatically remove dead addresses from list membership* control on the Members 433 screen of the Mailing List editor.

**List pruner saves messages which result in list member removal**
When MDaemon scans returned list messages in an attempt to remove member addresses that cannot be reached, this control will cause messages that result in a list member's removal to be saved.

**Honor '<List>-subscribe' and '<List>-unsubscribe' addresses**
Click this checkbox if you want MDaemon to recognize email addresses of this format as valid (as long as the list actually exists) in order to facilitate an easier method for users to join and leave your mailing lists. For example: suppose you have a list called `MyList@example.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@example.com` and `MyList-Unsubscribe@example.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Disable subaddressing feature for all accounts**
Click this option if you wish to globally disable the Subaddressing feature. Subaddressing will not be permitted for any account, regardless of the individual account settings. For more on Subaddressing, see the IMAP Filters 356 screen of the Account Editor.

**POP3, IMAP, and WorldClient passwords are case sensitive**
POP, IMAP, and WorldClient passwords will be case-sensitive when this control is checked.

**Inform postmaster when new MDaemon updates are available**
The option causes MDaemon to notify the postmaster whenever there is an MDaemon update available. The option is enabled by default.

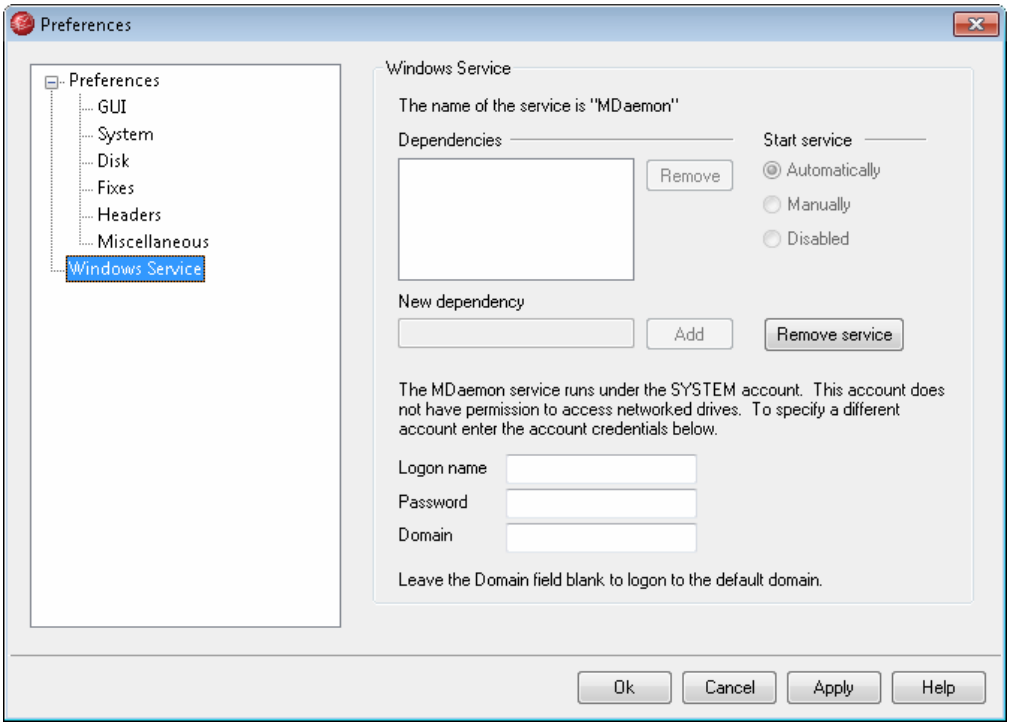
**No spam allowed in mailing list public folders**
By default, when a mailing list has an associated Public Folder 447, list messages will not be placed in that folder when their spam scores meet or exceed the value designated in the "*A message is spam if its score is greater or equal to*" option located on the Spam Filter 242 screen. Clear this checkbox if you wish to allow spam to be placed in the public folder.

**Send stats report to postmaster at midnight**
By default a statistics report will be sent to the postmaster each night at midnight. Clear this checkbox if you do not want the report to be sent. This option corresponds to the Statistics 31 tab located on MDaemon's main display.

**Account export includes disk usage stats (this could greatly slow export)**
By default, account exports do not include disk file counts and space consumed. If you wish to include this information in exports, enable this checkbox. This may, however, significantly slow export speeds.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 4.6.2 Windows Service




### Windows Service

When MDaemon is running as a service, the service's name is "MDaemon."

**Dependencies**
Use this option to designate any services what you wish to require to be running **before** the MDaemon service starts.

**Start service**
This is the initial state of the service: automatically starts, must be started manually, or disabled.

**Install/Remove service**
Click this button to install or remove the MDaemon service.

### Network Resource Access

When running MDaemon as a Windows service, by default it runs under the SYSTEM account. Because this account does not have access to network devices, MDaemon will not be able to access mail if you wish to store it on other computers across your LAN. That is, not unless you provide logon credentials for an account that can be used to provide the MDaemon service access to network shares. If you need to do this then you can create a Windows user account specifically designed for running MDaemon with whatever restrictions that you desire, but which has access to those network shares that you want MDaemon to be able to use. Further, all applications launched by MDaemon will use the same credentials.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Logon name**
This is the logon name of the Windows account under which the MDaemon service should run.

**Password**
This is the Windows account's password.

**Domain**
This is the Windows Domain on which the account resides. Leave this field blank to login to the default domain.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section V

# 5 Security Menu

MDaemon is equipped with an extensive suite of security features and controls. Click Security on MDaemon's menu bar to reach the following security features:

- **AntiVirus** 210 — SecurityPlus for MDaemon can help you stop email-borne computer viruses by providing the highest level of integrated protection available for MDaemon customers. It will catch, quarantine, repair, and/or remove any email message found to contain any virus. For MDaemon PRO users, SecurityPlus also contains a feature called Outbreak Protection, which can be used to protect you from certain spam, phishing, and virus outbreaks that can sometimes be missed by the other traditional, content and signature-based security measures.
- **Content Filter** 212 — a highly versatile and fully multi-threaded Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and much more.
- **Spam Filter** 241 — uses spam filtering technology to heuristically examine email messages in order to compute a "score". This score is used to determine the likelihood of a message being spam. Based on that determination the server can then take certain actions such as refusing or flagging the message. See also: Spam Traps 270
- **DNS Black Lists** 264 —allows you to specify several DNS blacklisting services that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these hosts, the message will be refused.
- **Relay Control** 271 — used to control what MDaemon will do when a message arrives at your mail server that is neither from nor to a local address.
- **IP Shield** 273 — if a domain name specified in this list attempts to connect to your server, its IP address must match the one that you have assigned to it.
- **Reverse Lookup** 275 — MDaemon can query DNS servers to check the validity of the domain names and addresses reported during incoming messages. Controls on this screen can be used to cause suspicious messages to be refused or a special header inserted into them. Reverse Lookup data will also be reported in the MDaemon logs.
- **POP Before SMTP** 278 — the controls on this screen are used to require each user to first access his or her mailbox before being allowed to send a message through MDaemon, thus authenticating that the user is a valid account holder and allowed to use the mail system.
- **Trusted Hosts** 279 — domain names and IP addresses that will be considered as exceptions to the relay rules listed on the Relay Control screen.
- **SMTP Authentication** 280 — used for setting several options that denote how MDaemon will behave when a user sending a message to MDaemon has or has not been authenticated first.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

- **SPF/Sender ID** 282 — All domains publish MX records to identify the machines that may receive mail for them, but this doesn't identify the locations allowed to send mail for them. Sender Policy Framework (SPF) and Sender ID is a means by which domains can also publish "reverse MX" records to identify those locations authorized to send messages.
- **DomainKeys and DomainKeys Identified Mail** 284 — DomainKeys (DK) and DomainKeys Identified Mail (DKIM) are email verification systems that can be utilized to prevent spoofing. They can also be used to ensure the integrity of incoming messages, ensuring that the message hasn't been tampered with between the time it left the sender's mail server and arrived at yours. This is accomplished by using an encrypted public/private key pairs system. Outgoing messages are signed using a private key and incoming messages have their signatures verified by testing them with the public key published on the sender's DNS server.
- **Certification** 294 — Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. The Certification feature is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It can also help lower the resources required to process each message.
- **Sender Blacklist** 299 — lists addresses that are not allowed to send mail traffic through your server.
- **IP Screen** 302 — used to designate IP addresses from which you will allow or refuse connections to your server.
- **Host Screen** 304 — used to designate hosts (domain names) from which you will allow or refuse connections to your server.
- **Dynamic Screen** 306 — using the Dynamic Screening feature, MDaemon can track the behavior of sending servers to identify suspicious activity and then respond accordingly. For example, you can temporarily ban an IP address from future connections to your server once a specified number of "unknown recipient" errors occur during the mail connection from that IP address.
- **SSL & TLS** 309 — MDaemon supports the Secure Sockets Layer (SSL) protocol for SMTP, POP, and IMAP, and for WorldClient's web server. SSL is the standard method for securing server/client Internet communications.
- **Backscatter Protection** 322 — "Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a Return-Path address that is forged. Backscatter Protection helps prevent this by ensuring that only legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the Return-Path address of your users' outgoing messages.
- **Bandwidth Throttling** 325 — the Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress, setting different rates for each of MDaemon's major services on a per-domain basis, including Domains and Domain Gateways.
- **Tarpitting** 328 — makes it possible for you to deliberately slow down a

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to send unsolicited bulk email to you. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to do so again in the future.

- **Greylisting** 330 — Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a non-white listed or otherwise previously unknown sender, its sender, recipient, and sending server's IP address will be logged and then the message will be refused by Greylisting with a temporary error code during the SMTP session. Then, when the legitimate servers attempt to deliver the messages again a few minutes later, they will be accepted. Because spammers do not typically make further delivery attempts, Greylisting can significantly help to reduce the amount of spam your users receive.
- **HashCash** 333 — HashCash is a "proof of work" system that is both an anti-spam tool and a Denial of Service countermeasure similar to an electronic form of postage. Using the HashCash system MDaemon can mint HashCash stamps, which are in effect "paid for" with CPU processing time rather than actual currency. A HashCash stamp is inserted into an outgoing message's headers and then verified by the recipient's email server and weighed according to the value of the stamp. Stamped messages are more likely to be legitimate and can therefore be passed through the receiving server's anti-spam systems.
- **LAN IPs** 336 — use this screen to list IP addresses that reside on your LAN (local area network). These IP addresses are therefore treated as local traffic for the purposes of bandwidth throttling, and may be exempt from various other security and spam prevention restrictions.
- **Site Policy** 337 — used for creating a site policy to be transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "This server does not relay."

## 5.1 Content Filter and AntiVirus

### Content Filter

The Content Filter 212 (Security » Content Filter) can be used for a large number of purposes such as: preventing spam email, intercepting messages containing viruses before they reach their final destination, copying certain emails to one or more additional users, appending a note or disclaimer to the bottom of messages, adding, and deleting headers, stripping email attachments, deleting messages, and more. Because individual Content Filter rules are created by the administrator, and because of their diversity, they can be used in many situations and are limited for the most part only be the creativity of the person creating them. With a little bit of thought and experimentation, this feature can be very useful.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## SecurityPlus for MDaemon

In a joint effort with Kaspersky Labs, a world-renowned anti-virus software developer, Alt-N Technologies has developed SecurityPlus for MDaemon, an anti-virus engine that can be installed and integrated with MDaemon. When SecurityPlus is installed you will see two additional tabs on the Content Filter dialog: AntiVirus 231 and AV Updater 233. These tabs are used to directly control the product's features and designate what actions MDaemon will take when a virus is detected. For MDaemon PRO users, SecurityPlus also contains a feature called Outbreak Protection 236, which is not heuristics-based or signature dependent like the traditional protection tools, but is designed to catch spam, phishing and virus attacks that are part of an ongoing outbreak, and which can sometimes by missed by the traditional tools. To obtain SecurityPlus for MDaemon, visit www.altn.com.

**See:**

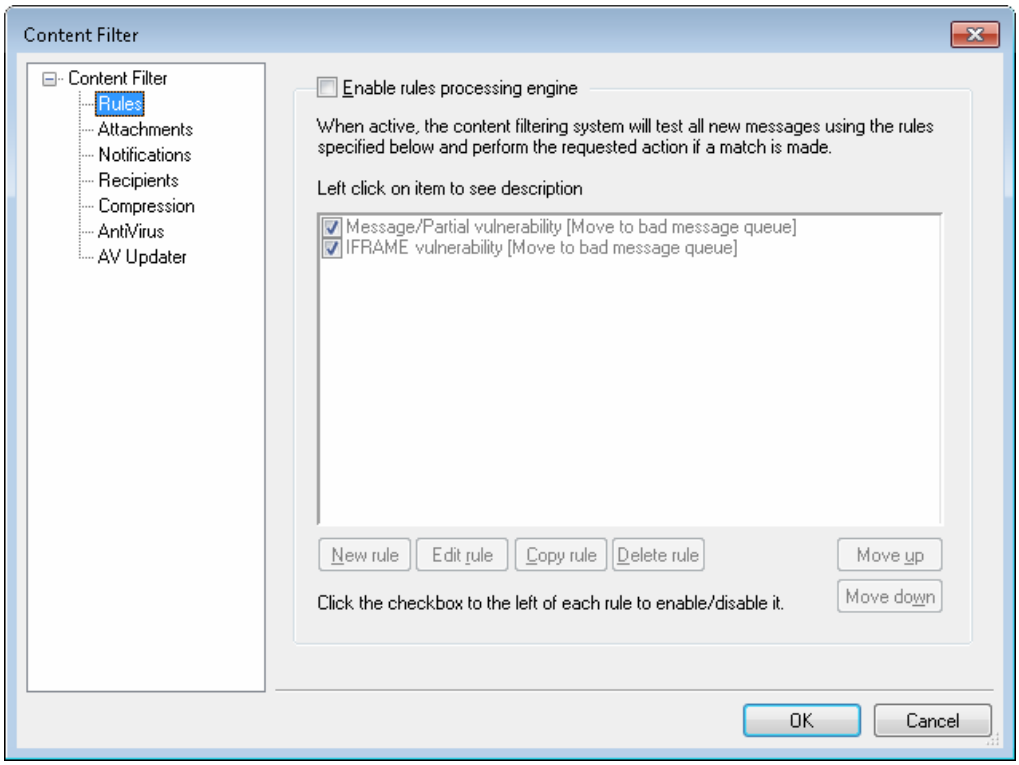
**Content Filter Editor** 212
**Creating a New Content Filter Rule** 214
**Modifying an Existing Content Filter Rule** 218
**Using Regular Expressions in Your Filter Rules** 218

**AntiVirus** 231
**AntiVirus Updater** 233
**Outbreak Protection** 236

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 5.1.1 Content Filter Editor

### 5.1.1.1 Rules




All messages processed by MDaemon will at some point reside temporarily in one of the message queues. When Content Filtering is enabled, before any message is allowed to leave the queue it will first be processed through the Content Filter rules. The result of this procedure will determine what is done with the message.

Messages that have a filename beginning with the letter "P" will be ignored by the content filtering process. Every other message will be processed through the content filter system. Once processed, MDaemon will change the first character of the filename to a "P". In this way a message will only be processed through the content filtering system once.

#### Content Filtering Rules

**Enable rules processing engine**
Click this checkbox to enable content filtering. All messages processed by MDaemon will be filtered through the content filter rules before being delivered.

#### Existing Content Filtering Rules

This box lists all of your Content Filter rules, with a checkbox beside each one so that you can enable/disable them at will. To see a description of any given rule in its internal script format, click that rule and pause your mouse-cursor over it

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

(moving your mouse will cause the description to disappear). Whenever a message is processed through the Content Filter, these rules will be applied in the order in which they are listed. This makes it possible for you to arrange your rules to achieve a greater level of versatility.

For example: If you have a rule that deletes all messages containing the words, "This is Spam!" and a similar rule that sends those messages to the Postmaster, then putting them in the right order will enable both rules to be applied to the message. This assumes that there isn't a "Stop Processing Rules" rule that applies to the message higher up in the list. If so, then you would use the *Move Up*/*Move Down* buttons to move the "Stop" rule below the other two. Then, any message containing "This is Spam!" would be copied to the Postmaster and then deleted.

MDaemon has the capability to create rules that will perform multiple tasks and use `and/or` logic. Considering the example above, instead of using multiple rules you could create a single rule that would accomplish all of those tasks and more.

**New rule**
Click this button to create a new content filter rule. This will open the Create Rule 214 dialog.

**Edit rule**
Click this button to open the selected rule in the Modify Rule 218 editor.

**Copy rule**
Click this button to clone the selected content filter rule. An identical rule will be created and added to the list. The new rule will be given a default name of "Copy of [Original Rule Name]". This is useful if you wish to create multiple similar rules. You can create a single rule, clone it several times, and then modify the copies as needed.

**Delete rule**
Click this button to delete the selected content filter rule. You will be asked to confirm your decision to delete the Rule before MDaemon will do so.

**Move up**
Click this button to move the selected rule up.

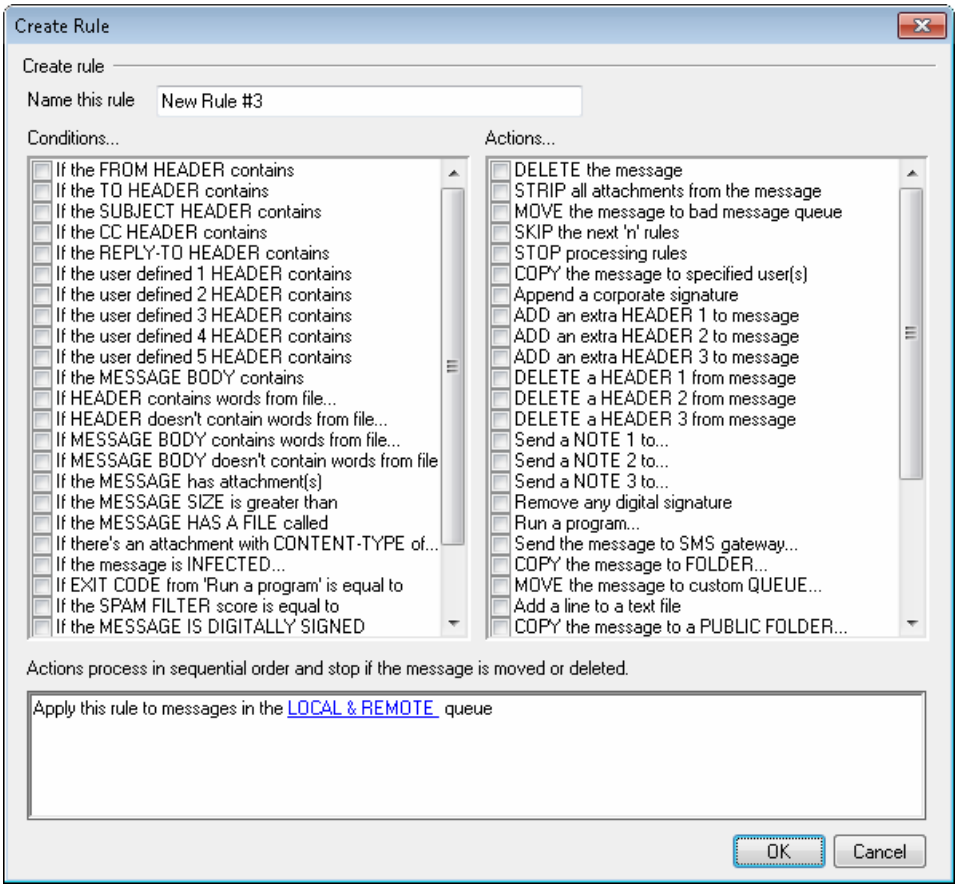
**Move down**
Click this button to move the selected rule down.

**See:**

**Creating a New Content Filter Rule** 214
**Modifying an Existing Content Filter Rule** 218
**Using Regular Expressions in Your Filter Rules** 218

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.1.1.1.1 Creating a New Content Filter Rule




This dialog is used for creating Content Filter Rules. It is reached by clicking the *New Rule* button on the Content Filter dialog.

#### Create Rule

**Name this rule**
Type a descriptive name for your new rule here. By default it will be called "New Rule #n".

#### Conditions...

This box lists the conditions that may be applied to your new rule. Click the checkbox corresponding to any condition that you want to be applied to the new rule. Each enabled condition will appear in the Rule Description box below. Most Conditions will require additional information that you will specify by clicking on the Condition's hyperlink in the Rule Description box.

**`If the [HEADER] contains`**—Click any of these options to base your rule on the content of those particular message headers. You must specify the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 218.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**If the user defined [# HEADER] contains**—Click one or more of these options to base the rule on message headers that you will define. You must specify the new header, and the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 218.

**If the MESSAGE BODY contains**—This option makes the contents of the message body one of the conditions. This condition requires you to specify a text string for which to search. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 218.

**If the MESSAGE has Attachment(s)**—When this option is selected, the rule will be contingent upon the presence of one or more message attachments. No additional information is required.

**If the MESSAGE SIZE is greater than**—Click this option if you want the rule to be based upon the size of the message. The size must be specified in *KB*. Default is 10KB.

**If the MESSAGE HAS A FILE called**—This option will scan for a file attachment with a particular name. The filename must be specified. Wildcards such as *.exe and file *.* are permitted.

**If message is INFECTED...**—This condition is `TRUE` when SecurityPlus for MDaemon determines that a message is infected with a virus.

**If the EXIT CODE from a previous run process is equal to**—If a previous rule in your list utilizes the *Run Process* action, you can use this condition to look for a specific exit code from that process.

**If the MESSAGE IS DIGITALLY SIGNED**—The condition applies to messages that have been digitally signed. No further information is required by this condition.

**If SENDER is a member of GROUP...**—This condition applies to a message when it is sent by an account that is a member of the account Group designated in the rule.

**If RECIPIENT is a member of GROUP...**— This condition applies to a message when its recipient is a member of the account Group designated in the rule.

**If ALL MESSAGES**—Click this option if you want the rule to be applied to all messages. No further information is required; this rule will affect every message except those to which a "Stop Processing Rules" or "Delete Message" action has been applied in a previous rule.

### Actions...

MDaemon can perform these actions if a message matches the rule's conditions. A few Actions will require additional information that you will specify by clicking on the Action's hyperlink in the Rule Description box.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Delete Message**—Selecting this action will cause the message to be deleted.

**Strip All Attachments From Message**—This action causes all attachments to be stripped from the message.

**Move Message To Bad Message Directory**—Click this action to cause a message to be moved to the bad message directory.

**Skip n Rules**—Selecting this action will cause a specified number of rules to be skipped. This is useful in situations where you may want a rule to be applied in certain circumstances but not in others.

For example: you may wish to delete messages that contain the word "Spam", but not those that contain "Good Spam". To accomplish this you could create a rule that deletes messages containing "Spam" and then place above it another rule that states "if the message contains "Good Spam" then Skip 1 Rule".

**Stop Processing Rules**—This action will skip all remaining rules.

**Copy Message To Specified User(s)**—Causes a copy of the message to be sent to one or more recipients. You must specify which recipients are to receive the message.

**Append Standard Disclaimer**—This action makes it possible for you to create a small amount of text that will be appended as a footer to the message. Alternatively, it can add the contents of a text file.

For example: you could use this rule to include a statement that says "This email originated from my company, please direct any complaints or questions to user01@example.com".

**Add Extra Header Item To Message**—This action will add an additional header to the message. You must specify the name of the new header and its value.

**Delete A Header Item From Message**—This action will remove a header from a message. You must specify the header that you wish to delete.

**Send Note To...** —This action will send an email to a particular address. You will be able to specify the recipient, sender, subject, and a small amount of text. You can also configure this action to attach the original message to the note.

For example: you might wish to create a rule that will move all messages containing "This is Spam!" to the bad message directory and create another rule that will send a note to someone letting them know that this has been done.

**Remove Digital Signature**—Click this action to cause a digital signature to be removed from the message.

**Run Process...**—This action can be used to run a particular program when a

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

message meets the rule's conditions. You must specify the path to the program that you wish to run. You can use the $MESSAGEFILENAME$ macro to pass the name of the message to the process, and you can specify whether or not MDaemon should suspend its operations temporarily or indefinitely while it waits for the process to terminate. Further, you can force the process to terminate and/or run it in a hidden window.

**Send Message Through SMS Gateway Server...**—Click this option to send the message through an SMS Gateway Server. You must supply the Host or IP Address and the SMS phone number.

**Copy Message to Folder...**—Use this option to place a copy of the message into a specific folder.

**MOVE the messages to custom QUEUE...**—Use this action to move the message into one or more previously created custom mail queues. When moving messages to custom remote mail queues you can use the custom scheduling options on the Event Scheduler to control when those messages will be processed.

**Add Line To Text File**—This option will cause a line of text to be added to a specific text file. When choosing this action you will have to specify the path to the file and the text that you want to be appended to it. You may use certain MDaemon macros in your text to cause the content filter to dynamically include information about the message such as the sender, recipient, message ID, and so on. Click the Macros button on the "Add line to text file" dialog to display a list of permitted macros.

**Move Message to Public Folders...**—Use this action to cause the message to be moved to one or more Public Folders.

**Search and Replace Words in a Header**—Use this option to scan a specified header for certain words and then delete or replace them. When creating this rule, click the "specify information" link in the Rule Description to open the "Header – Search and Replace" dialog on which you will designate the header and words to replace or delete. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 218.

**Search and Replace Words in the Message Body**—Use this option to scan the message body and replace any desired text. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 218.

**Jump to Rule...**—Use this action to jump immediately to a rule further down in the list, skipping over all rules between the two.

**Sign with DomainKeys selector...**—Use this action if you want the rule to cause a message to contain a DomainKeys signature 289. You can also use it if you wish to sign some messages using a selector other than the one designated on the DK & DKIM dialog.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Sign with DKIM selector...**—Use this action if you want the rule to cause a message to contain a DKIM signature[289]. You can also use it if you wish to sign some messages using a selector other than the one designated on the DK & DKIM dialog.

**Rule description**
This box displays the new rule's internal script format. Click any of the rule's conditions or actions (listed as hyperlinks) and the appropriate editor will be opened for specifying any needed information.

**See:**

**Content Filter Editor**[212]
**Modifying an Existing Content Filter Rule**[218]
**Using Regular Expressions in Your Filter Rules**[218]

### 5.1.1.1.2 Modifying an Existing Content Filter Rule

To modify an existing content filter rule, select the rule and then click the *Edit Rule* button on the Content Filter dialog. The rule will be opened for editing in the Modify Rule editor. The controls on this editor are identical to the Create Rule Dialog[214].

**See:**

**Content Filter Editor**[212]
**Creating a New Content Filter Rule**[214]
**Using Regular Expressions in Your Filter Rules**[218]

### 5.1.1.1.3 Using Regular Expressions in Your Filter Rules

The Content Filtering system supports *regular expression* searches, which is a versatile system that makes it possible for you to search not only for specific text strings, but also for text *patterns*. Regular expressions contain a mix of plain text and special characters that indicate what kind of matching to do, and can thus make your Content Filter rules more powerful and better targeted.

**What are Regular Expressions?**
A regular expression (regexp) is a text pattern consisting of a combination of special characters known as *metacharacters* and alphanumeric text characters, or "*literals*" (abc, 123, and so on). The pattern is used to match against text strings—with the result of the match being either successful or not. Regexps are used primarily for regular text matches and for search and replace.

Metacharacters are special characters that have specific functions and uses within regular expressions. The regexp implementation within the MDaemon Content Filtering system allows the following metacharacters:

```
\ | () [] ^ $ * + ? . <>
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| Metacharacter | Description |
|---|---|
| **** | When used before a metacharacter, the backslash ( "\" ) causes the metacharacter to be treated as a literal character. This is necessary if you want the regular expression to search for one of the special characters that are used as metacharacters. For example, to search for "+" your expressions must include "\+". |
| **\|** | The *alternation* character (also called "*or*" or "*bar*") is used when you want either expression on the side of the character to match the target string. The regexp "abc\|xyz" will match any occurrence of either "abc" or "xyz" when searching a text string. |
| **[...]** | A set of characters contained in brackets ("[" and "]") means that any character in the set may match the searched text string. A dash ("-") between characters in the brackets denotes a range of characters. For example, searching the string "abc" with the regexp "[a-z]" will yield three matches: "*a*," "*b*, " and "*c*. " Using the expression "[az]" will yield only one match: "*a*." |
| **^** | Denotes the beginning of the line. In the target string, "abc ab a" the expression "^a" will yield one match—the first character in the target string. The regexp "^ab" will also yield one match—the first *two* characters in the target string. |
| **[^...]** | The caret ("^") immediately following the left-bracket ("[") has a different meaning. It is used to exclude the remaining characters within brackets from matching the target string. The expression "[^0-9]" indicates that the target character should not be a digit. |
| **(...)** | The parenthesis affects the order of pattern evaluation, and also serves as a *tagged* expression that can be used in *search and replace* expressions.<br><br>The results of a search with a regular expression are kept temporarily and can be used in the *replace* expression to build a new expression. In the *replace* expression, you can include a "&" or "\0" character, which will be replaced by the sub-string found by the regular expression during the search. So, if the *search* expression "a(bcd)e" finds a sub-string match, then a *replace* expression of "123-&-123" or "123-\0-123" will replace the matched text with "123-abcde-123".<br><br>Similarly, you can also use the special characters "\1," "\2," "\3," and so on in the *replace* expression. These characters will be replaced only be the results of the *tagged* expression |

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

instead of the entire sub-string match. The number following the backslash denotes which tagged expression you wish to reference (in the case of a regexp containing more than one tagged expression). For example, if your *search* expression is "(123)(456)" and your *replace* expression is "a-\2-b-\1" then a matching sub-string will be replaced with "a-456-b-123" whereas a *replace* expression of "a-\0-b" will be replaced with "a-123456-b"

**$** The dollar sign ("$") denotes the end of the line. In the text string, "13 321 123" the expression "3$" will yield one match —the last character in the string. The regexp "123$" will also yield one match—the last *three* characters in the target string.

***** The asterisk ("*") quantifier indicates that the character to its left must match *zero or more* occurrences of the character in a row. Thus, "1*abc" will match the text "111abc" and "abc."

**+** Similar to the asterisk quantifier, the "+" quantifier indicates that the character to its left must match *one or more* occurrences of the character in a row. Thus, "1+abc" will match the text "111abc" but not "abc."

**?** The question mark ("?") quantifier indicates that the character to its left must match *zero or one* times. Thus, "1*abc" will match the text "abc," and it will match the "1abc" portion of "111abc."

**.** The period or dot (".") metacharacter will match any other character. Thus ".+abc" will match "123456abc," and "a.c" will match "aac," abc," acc," and so on.

**Eligible Conditions and Actions**
Regular expressions may be used in any *Header* filter rule *Condition*. For example, any rule using the "`if the FROM HEADER contains`" condition. Regular expressions may also be used in the "`if the MESSAGE BODY contains`" condition.

Regular expressions may be used in two Content Filter rule *Actions*: "`Search and Replace Words in a Header`" and "`Search and Replace Words in the Message Body`."

Regular expressions used in Content Filter rule *conditions* are case insensitive. Case will not be considered.

Case sensitivity in regular expressions used in Content Filter rule *actions* is optional. When creating the regexp within the rule's action you will have the option to enable/disable case sensitivity.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Configuring a Regexp in a Rule's Condition

To configure a header or message body condition to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the header or message body condition that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**contains specific strings**" link that corresponds to the condition that you selected in step 1. This will open the Specify Search Text dialog.

3. Click the "**contains**" link in the "Currently specified strings..." area.

4. Choose "**Matches Regular Expression**" from the drop-down list box, and click **OK**.

5. If you need help creating your regexp or want to test it then click "**Test regular expression**." If you do not need to use the Test Regular Expression dialog then type your regexp into the text box provided, click **Add**, and then go to step 8.

6. Type your regular expression into the "Search expression" text box. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu. When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

7. Type any text that you wish to use to test your expression in the text area provided, and click **Test**. When you are finished testing your expression, click **OK**.

8. Click **OK**.

9. Continue creating your rule normally.

### Configuring a Regexp in a Rule's Action

To configure a "Search and Replace Words in…" action to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the "*Search and Replace Words in...*" action that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**specify information**" link that corresponds to the action that you selected in step 1. This will open the Search and Replace dialog.

3. If you chose the "*Search...header*" action in step 1, then use the drop-down list box provided to choose the header that you wish to search, or type a header into the box if the desired header isn't listed. If you did not choose the "*Search... header*" action in step 1 then skip this step.

4. Type the *search* expression that you wish to use in this action. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

5. Type the *replace* expression that you wish to use in this action. As with the *search* expression we have provided a metacharacter shortcut menu for this option as well. Leave this text box blank if you wish to delete a matched sub-string instead of replace it with more text.

6. Click "**Match case**" if you want the expression to be case sensitive.

7. Click Regular expression if you want the search and replace strings to be treated as regular expressions. Otherwise each will be treated as a simple sub-string search and replace—it will look for an exact literal match of the text rather than process it as a regular expression.

8. If you do not need to test your expression then skip this step. If you do need to test your expression then click "**Run Test**." On the Search and Replace Tester dialog, type your search and replace expressions and the text that you wish to test with, then click **Test**. When you are finished testing your regexps click **OK**.

9. Click **OK**.

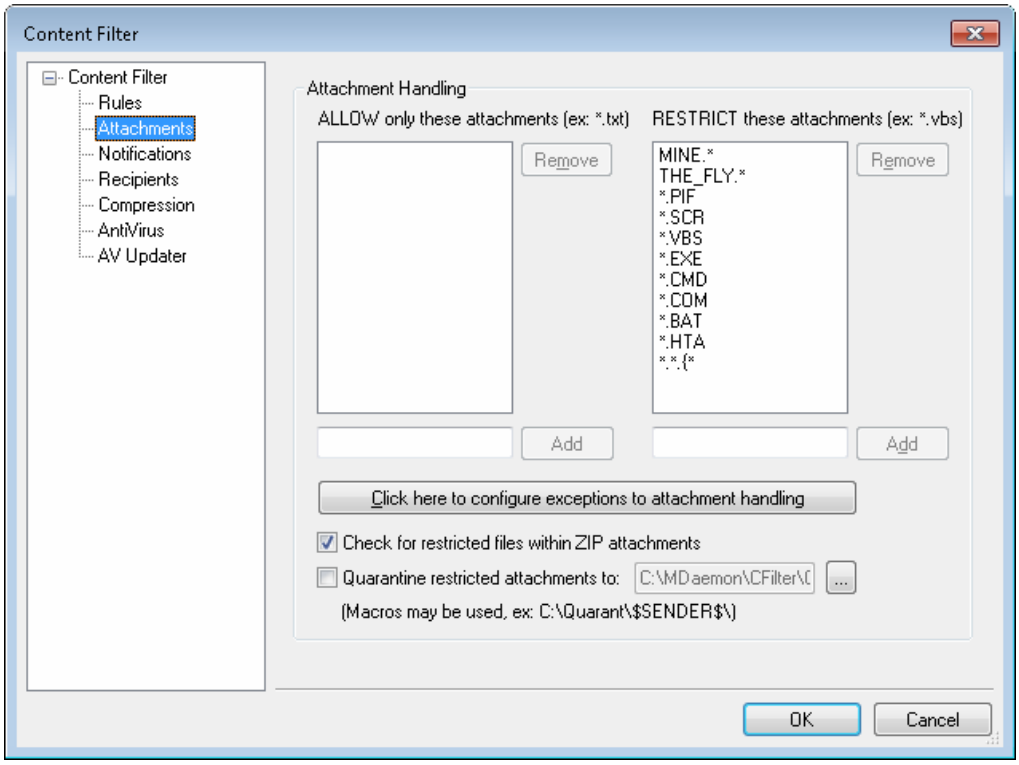
10. Continue creating your rule normally.

MDaemon's regexps implementation uses the PERL Compatible Regular Expression (PCRE) library. You can find more information on this implementation of regexps at: http://www.pcre.org/ and http://perldoc.perl.org/perlre.html.

For a comprehensive look at regular expressions, see: *Mastering Regular Expressions, Third Edition* published by O'Reilly Media, Inc.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.1.1.2 Attachments




Use this tab to specify attachments that you wish to classify as allowed or restricted. Attachments that are not allowed will be automatically removed from messages.

**Attachment Handling**

Filenames specified in *RESTRICT these attachments* list will be stripped from messages automatically when MDaemon encounters them. If you list any files in the *ALLOW only these attachments* list, then only those files listed will be permitted — all other attachments will be stripped from messages. After the attachment is stripped, MDaemon will continue normally and delivery the message without it. You can use the options on the Notifications tab to cause a notification message to be sent to various addresses when one of these restricted attachments is encountered.

Wildcards are permitted in list entries. An entry of "`*.exe`", for example, would cause all attachments ending with the `EXE` file extension to be allowed or removed. To add an entry to either of the lists, type the filename in the space provided and the click Add.

**Click here to configure exceptions to attachment handling**
Click this button to specify addresses that you wish to exclude from attachment restriction monitoring. When a message is directed to one of these addresses MDaemon will allow the message to pass even if it contains a restricted attachment.

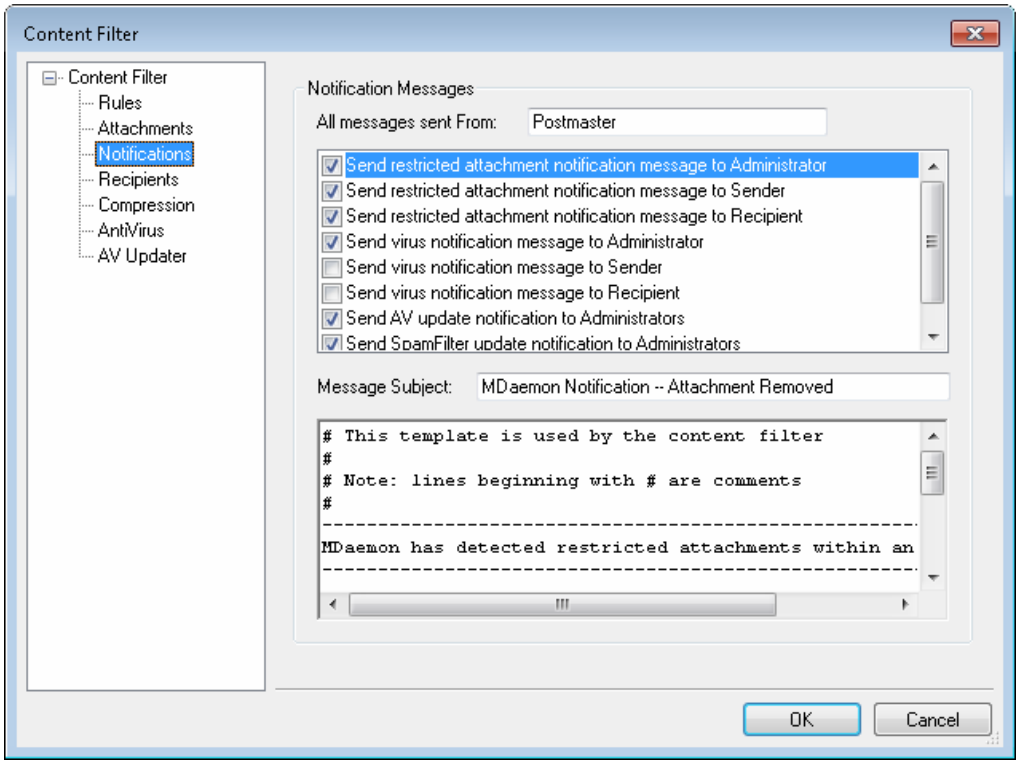
**Check for restricted files within ZIP attachments**
Click this option if you wish to scan the contents of zipped files for restricted attachments. Additionally, any Content Filter rule set to look for a particular

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

filename will be triggered if a matching file is found within a zipped attachment.

**Quarantine restricted attachments to:**
Click this option and specify a location if you wish to quarantine restricted attachments to a specific location rather than simply delete them.

### 5.1.1.3 Notifications




Used this tab to designate those who should receive notification messages when a virus or restricted attachment is detected.

#### Notification Messages

**All messages sent From:**
Use this box for specifying the address from which you wish the notification messages to be sent.

**Send virus notification message to...**
When a message arrives with a file attachment containing a virus, a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Send restricted attachment notification message to...**
When a message arrives with a file attachment matching a restricted attachment entry (listed on the Attachments tab) a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

**Message Subject:**
This text will be displayed in the "Subject:" header of the notification message that is sent.

**Message**
This is the message that will be sent to the entry selected in the list above when the checkbox corresponding to that entry is enabled. You can directly edit this message from the box in which it is displayed.

The actual files containing this text are located in the `MDaemon\app\` directory. They are:

`cfattrem[adm].dat` – Restricted attachment message – Admins
`cfattrem[rec].dat` – Restricted attachment message – Recipient
`cfattrem[snd].dat` – Restricted attachment message – Sender
`cfvirfnd[adm].dat` – Virus found message – Admins
`cfvirfnd[rec].dat` – Virus found message – Recipient
`cfvirfnd[snd].dat` – Virus found message – Sender

Should you desire to restore one of these messages to its original appearance, simply delete the relevant file and MDaemon will recreate it in its default state.

### 5.1.1.3.1 Message Macros

For your convenience, certain macros may be used in the notification messages and other messages that the Content Filters generate. You may use any of the following macros:

`$ACTUALTO$` Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro is replaced with that

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

value.

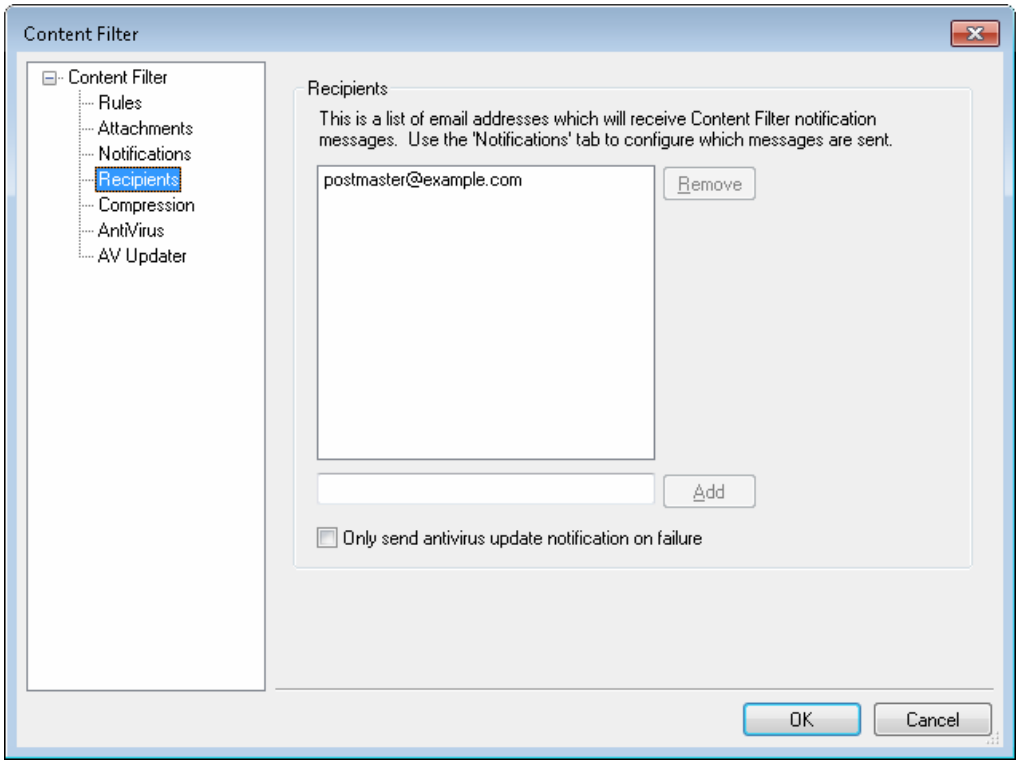
| | |
|---|---|
| $AV_VERSION$ | Lists the version of SecurityPlus for MDaemon that you are using. |
| $CURRENTTIME$ | This macro is replaced with the current time when the message is being processed. |
| $ACTUALFROM$ | Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro is replaced with that value. |
| $FILTERRULENAME$ | This macro is replaced by the name of the rule whose criteria the message matched. |
| $GEN_GUID$ | Generates a unique ID with 11 alpha-numeric characters. Example: 0XVBASADTZC |
| $HEADER:XX$ | This macro will cause the value of the header specified in place of the "xx" to be expanded in the reformatted message. For example: If the original message has "TO: user01@example.com" then the $HEADER:TO$ macro will expand to "user01@example.com". If the original message has "Subject: This is the subject" then the $HEADER:SUBJECT$ macro would be replaced with the text "This is the subject" |
| $HEADER:MESSAGE-ID$ | As with $HEADER:XX$ above, this macro will expand to the value of the Message-ID header. |
| $LIST_ATTACHMENTS_REMOVED$ | When one or more attachments are removed from the message, this macro will list them. |
| $LIST_VIRUSES_FOUND$ | When one or more viruses is found in a message, this macro will list them. |
| $MESSAGEFILENAME$ | This macro expands to the file name of the current message being processed. |
| $MESSAGEID$ | As $HEADER:MESSAGE-ID$ above, except this macro strips "<>" from the value of the message ID. |
| $PRIMARYDOMAIN$ | Expands to MDaemon's Default Domain name, which is designated on the Default Domain Configuration dialog (click Setup→Default Domain). |
| $PRIMARYIP$ | This macro expands to the IP address of your Default Domain (specified on the Default Domain Configuration dialog) |
| $RECIPIENT$ | This macro resolves to the full address of the |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

message recipient.

| | |
|---|---|
| $RECIPIENTDOMAIN$ | This macro will insert the domain name of the message recipient. |
| $RECIPIENTMAILBOX$ | Lists the recipient's mailbox (the value to the left of "@" in the email address). |
| $REPLYTO$ | This macro expands to the value of the message's "Reply-to" header. |
| $SENDER$ | Expands to the full address from which the message was sent. |
| $SENDERDOMAIN$ | This macro will insert the domain name of the message's sender (the value to the right of "@" in the email address). |
| $SENDERMAILBOX$ | Lists the sender's mailbox (the value to the left of "@" in the email address). |
| $SUBJECT$ | Displays the text contained in the message's subject. |

### 5.1.1.4 Recipients




**Recipients**

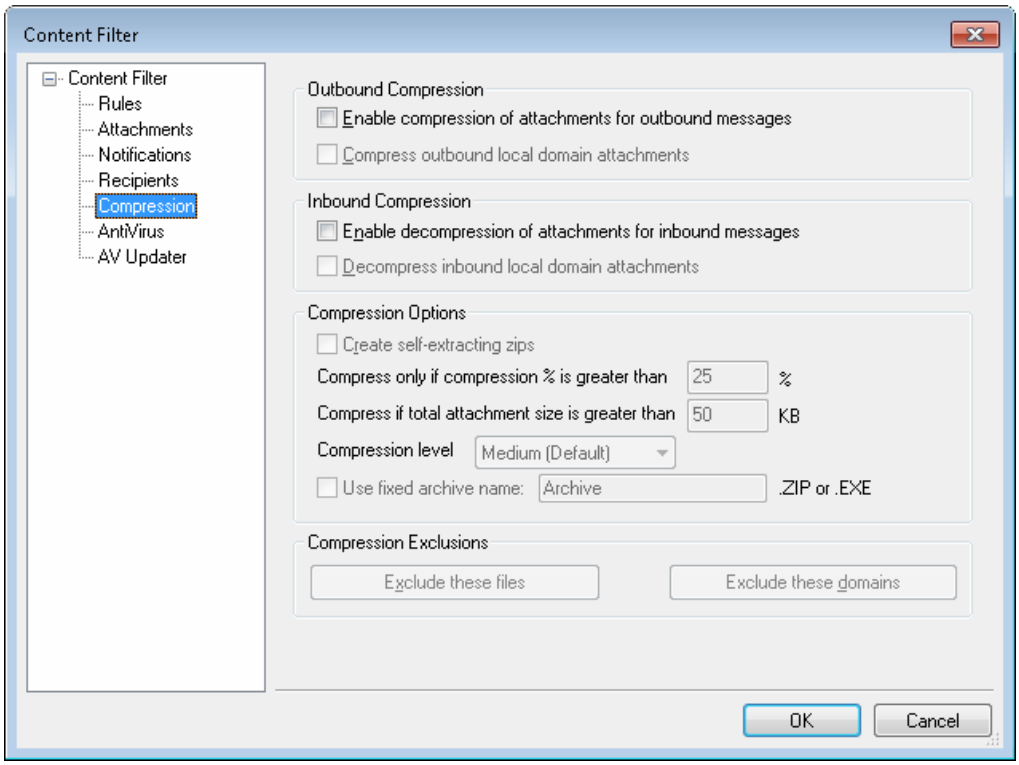
This list of recipients corresponds to the various "*send...to administrator*" options

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

located on the Notifications tab. These addresses will receive notification messages when one of the Administrator options is selected on that tab. To add an address to this section, type it into the space provided and then click *Add*. To remove an address, select it from the list and then click *Remove*.

**Only send antivirus update notification on failure**
Click this checkbox if you wish to send antivirus update notification messages only when the update attempt fails for some reason.

### 5.1.1.5 Compression




With the controls on this tab you can cause message attachments to be automatically compressed or decompressed before the message is delivered. The level of compression can be controlled as well as several other parameters and exclusions. This feature could significantly reduce the amount of bandwidth and throughput required to deliver your outbound messages.

#### Outbound Compression

**Enable compression of attachments for outbound messages**
Click this checkbox if you want to enable automatic message attachment compression for outbound remote mail messages. Enabling this control will not cause all message attachments to be compressed; it simply turns the feature on. Whether an outbound message's files are compressed or not is determined by the remaining settings on this tab.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Compress outbound local domain attachments**
Enabling this control will cause the file compression settings to be applied to all outbound mail – even those messages whose destination is another local address.

## Inbound Compression

**Enable decompression of attachments for inbound messages**
Click this checkbox if you want to enable automatic decompression of inbound remote mail message attachments. When a message arrives with a zipped attachment, MDaemon will decompress it before delivering it to the local user's mailbox.

**Decompress inbound local domain attachments**
Enable this control if you want automatic decompression to apply to local mail as well.

## Compression Options

**Create self-extracting zips**
Click this checkbox if you want the compression files that MDaemon creates to be self-extracting zip files with an `EXE` file extension. This is useful if you are concerned that the message recipients may not have access to a decompression utility. Self-extracting zip files can be decompressed simply by double-clicking on them.

**Compress only if compression % is greater than XX%**
MDaemon will not compress a message's attachments before sending it unless they can be compressed by a percentage greater than the value specified in this control. For example, if you designate a value of 20 and a given attachment can't be compressed by at least 21% then MDaemon will not compress it before sending the message.

MDaemon must first compress a file to determine by what percentage it can be compressed. Thus, this feature does not prevent files from being compressed – it simply prevents file attachments from being sent in a compressed format when they cannot be compressed beyond the designated value. In other words, if after compressing the file MDaemon finds that it couldn't be compressed by more than this value, the compression will be disregarded and the message will be delivered with its attachments unchanged.

**Compress if total attachment size is greater than XX KB**
When automatic attachment compression is enabled, MDaemon will only attempt to compress a message's attachments when their total size exceeds the value specified here. Messages with total attachment sizes below this threshold will be delivered normally with the attachments unchanged.

**Compression level**
Use the drop-down list box to choose the degree of compression that you want

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

MDaemon to apply to automatically compressed attachments. You can choose three levels of compression: minimum (fastest compression process with least compression), medium (default value), or maximum (slowest compression process but highest degree of compression).

**Use fixed archive name: [archive name]**
Click this checkbox and choose a name if you want the automatically compressed attachments to have a specific filename.

### Compression exclusions

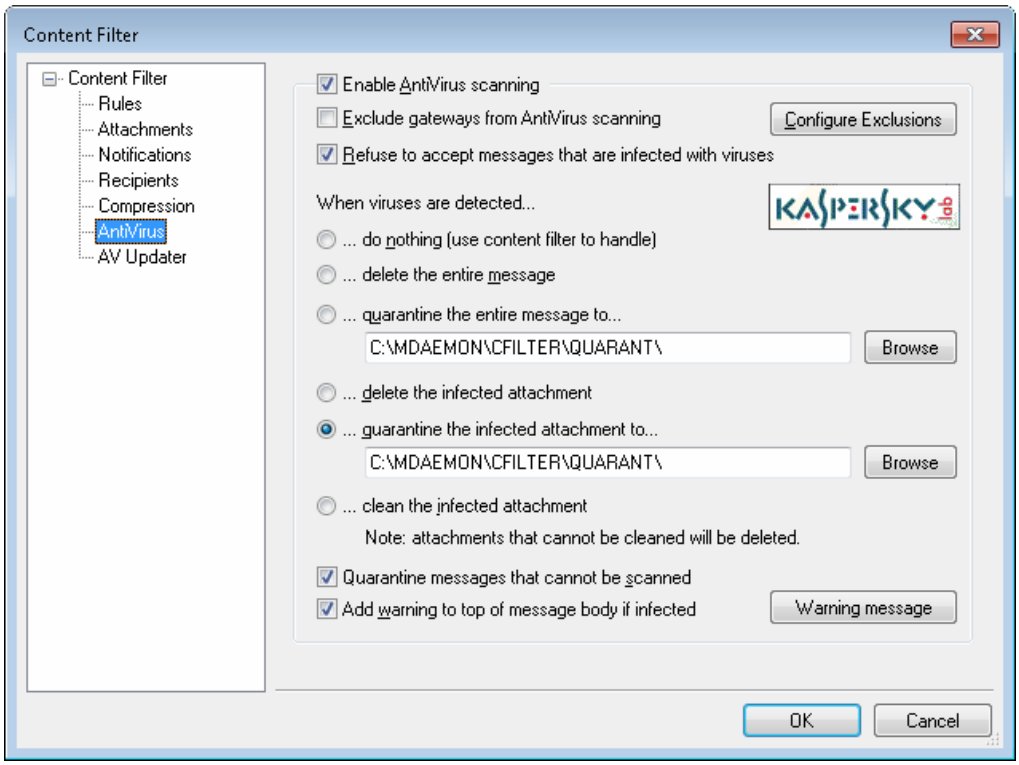
**Exclude these attachments...**
Click this button to specify files that you want to exclude from the automatic compression features. When a message attachment matches one of these filenames it will not be compressed, regardless of the compression settings. Wildcards are permitted in these entries. Therefore, you could specify "*.exe", for example, and all files ending with ".exe" would remain uncompressed.

**Exclude these domains...**
Click this button to specify recipient domains whose messages you wish to exclude from automatic compression. Messages bound for these domains will not have their file attachments compressed, regardless of your compression settings.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 5.1.2 AntiVirus

### 5.1.2.1 AntiVirus




This tab (and the AntiVirus Updater tab 233) will only be visible when you have installed SecurityPlus for MDaemon. To obtain SecurityPlus for MDaemon, visit www.altn.com.

#### Scanner Configuration

**Enable AntiVirus scanning**
Click this checkbox to enable AntiVirus scanning of messages. When MDaemon receives a message with attachments, it will activate SecurityPlus for MDaemon and scan them for viruses before delivering the message to its final destination.

**Exclude gateways from virus scanning**
Click this checkbox if you want messages bound for one of MDaemon's domain gateways to be excluded from virus scanning. This may be desirable for those who wish to leave the scanning of those messages to the domain's own mail server. For more information on domain gateways, see Domain Gateways 458.

**Refuse to accept messages that are infected with viruses**
Click this option is you wish to scan incoming messages for viruses during the SMTP session rather than after the session is concluded, and then reject those messages found to contain viruses. Because each incoming message is scanned before MDaemon officially accepts the message and concludes the session, the sending server is still responsible for it—the message hasn't technically been delivered yet. Thus the message can be rejected outright when a virus is found. Further, because the message was rejected, no further AntiVirus related actions listed on this dialog

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

will be taken. No quarantine or cleaning procedures will be taken, and no notification messages will be sent. This can greatly reduce the number of infected messages and virus notification messages that you and your users receive.

The SMTP-(in) log will show the result of AV processing. The possible results you might see are:

- the message was scanned and found infected with a virus
- the message was scanned and no virus was found
- the message could not be scanned (usually because a ZIP or other type or attachment could not be opened/accessed)
- the message could not be scanned (it exceeds the max size limit)
- an error occurred during the scan

**Configure Exclusions**
Click the Configure Exclusions button to specify recipient addresses to exclude from virus scanning. Messages bound for these addresses will not be scanned for viruses by SecurityPlus for MDaemon. Wildcards are allowed in these addresses. You could therefore use this feature to exclude entire domains or specific mailboxes across all domains. For example, "*@example.com or "VirusArchive@*".

**When viruses are detected...**
Click one of the options in this section to designate the action that MDaemon will take when SecurityPlus for MDaemon detects a virus.

**...do nothing (use content filter to handle)**
Choose this option if you wish to take none of the above actions, and have set up content filter rules to take some alternative actions instead.

**...delete the entire message**
This option will delete the entire message rather than just the attachment when a virus is found. Because this deletes the whole message, the "*Add a warning...*" option doesn't apply. However, you can still send a notification message to the recipient by using the controls on the Notifications tab.

**...quarantine the entire message to...**
This option is like the "*Delete the entire message*" option above, but the message will be quarantined in the specified location rather than deleted.

**...delete the infected attachment**
This option will delete the infected attachment. The message will still be delivered to the recipient but without the infected attachment. You can use the "*Add a warning...*" control on the bottom of this dialog to add text to the message informing the user that an infected attachment was deleted.

**...quarantine the infected attachment to...**
Choose this option and specify a location in the space provided if you want infected attachments to be quarantined to that location rather than deleted or cleaned. Like the "*Delete the infected attachment*" option, the message will still be

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

delivered to the recipient but without the infected attachment.

**...clean the infected attachment**
When this option is chosen, SecurityPlus for MDaemon will attempt to clean (i.e. disable) the infected attachment. If the attachment cannot be cleaned, it will be deleted.

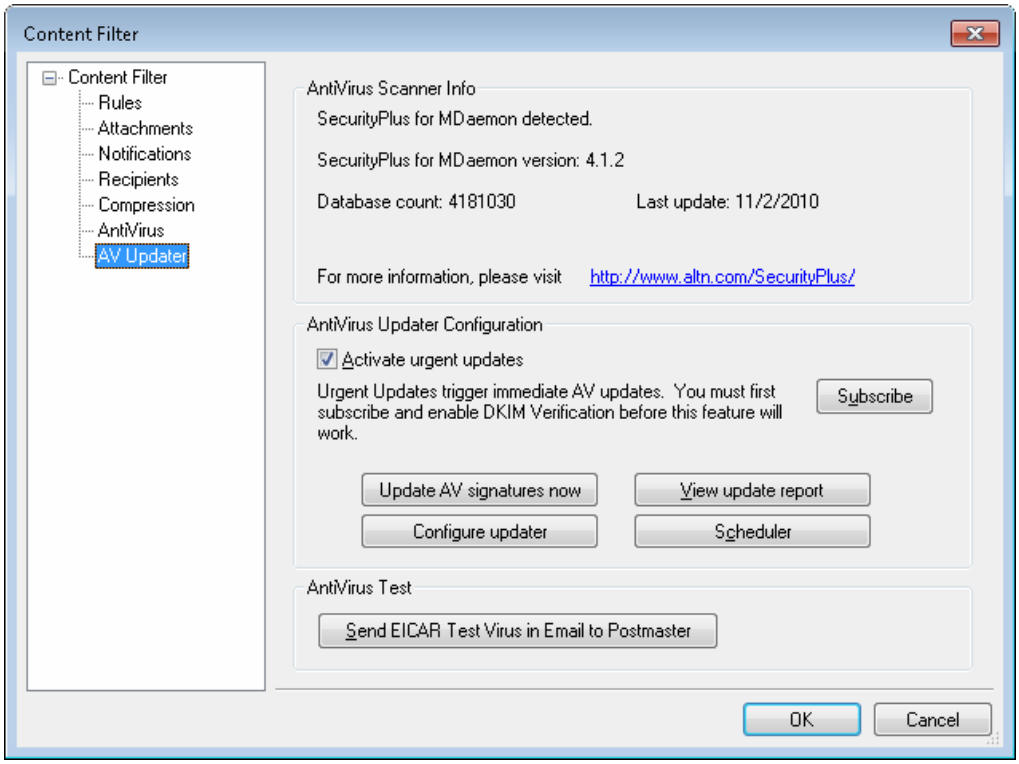
**Add warning to top of message body if infected**
When one of the "*...attachment*" options is chosen above, click this option if you want to add some warning text to the top of the previously infected message before it is delivered to the recipient. Thus you can inform the recipient that the attachment was stripped and why.

**Warning message...**
Click this button to display the warning text that will be added to messages when the "*Add a warning message...*" feature is used. After making any desired changes to the text, click "OK" to close the dialog and save the changes.

**See:**

**AV Updater** 233
**Content Filter and SecurityPlus** 210

### 5.1.2.2 AV Updater




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Use the controls on this tab to manually or automatically update SecurityPlus for MDaemon's virus definitions. There is a scheduler for automatic updating, a report viewer so that you can review when and which updates have been downloaded, and a test feature used for confirming that you your virus scanning is working properly.

### AntiVirus Scanner Info

This section tells you whether SecurityPlus for MDaemon is installed and, if so, what version you are running. It also lists the date of your last virus definition update.

### AntiVirus Updater Configuration

**Activate urgent updates**
Click this checkbox to activate the urgent updates feature. With this feature enabled, SecurityPlus will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message. To receive these messages you must first subscribe to the "Urgent Updates" feature. See the *Subscribe* option below.

**Subscribe**
This button opens your default browser to Alt-N Technologies' Urgent Updates subscription page. On that page enter your domain name to subscribe your domain to the Urgent Updates mailing list. Whenever there is an urgent update to SecurityPlus for MDaemon's virus definitions, an email will be dispatched to the domain. When MDaemon receives the message, SecurityPlus will be updated immediately.

**Update AV signatures now**
Click this button to update the virus definitions manually. The updater will connect immediately after the button is pressed.

**Configure updater**
Click this button to open the Updater Configuration dialog 235. This dialog contains four tabs: Update URLs, Connection, Proxy, and Misc.

**View update report**
The SecurityPlus Log Viewer is opened by clicking the *View update report* button. The viewer lists the times, actions taken, and other information about each update.

**Scheduler**
Click this button to open MDaemon's Event Scheduler to the AntiVirus Updates 151 screen, used for scheduling checks for virus signature updates at specific times on specific days or at regular intervals. There is also an *Activate urgent updates* option on that screen that can be used to activate or deactivate Automatic Urgent Updates. That option is the same as the control of the same name described above.

### AntiVirus Test

**Send EICAR Test Virus in Email to Postmaster**
Click this button to send a test message to the postmaster, with the EICAR virus file attached. This attachment is harmless – it is merely used to test SecurityPlus for MDaemon. By watching the Content Filter's log window on MDaemon's main interface

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

you can see what MDaemon does with this message when it is received. For example, depending upon your settings, you might see a log excerpt that looks something like the following:

```
Mon 2008-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2008-02-25 18:14:49: > Message from: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID: <MDAEMON10001200202251814.
AA1447619@example.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1 (including
multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (sender)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

**See:**

**Updater Configuration Dialog** 235
**AntiVirus** 231
**Content Filter and SecurityPlus** 210

### 5.1.2.2.1 Updater Configuration Dialog

Click the *Configure updater* button on the AV Updater tab 233 to open the Updater Configuration dialog. It contains the following four tabs:

**Update URLs**
The Update URLs tab is used to designate the servers that SecurityPlus for MDaemon will check for updates. You can choose to let SecurityPlus manage these URLs automatically or manually enter them yourself.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Connection**
The Connection tab is used to designate the Internet Connection Profile that you wish SecurityPlus to use when connecting to the update sites. The "*Use Internet Settings from Control Panel*" option uses your default Internet settings. The "*Setup Internet settings manually*" option and subsequent controls can be used to manually choose a Connection Profile and designate its user name and password settings.

**Proxy**
The Proxy tab contains options for configuring any HTTP or FTP proxy settings that your current network configuration may require in order to connect to the update sites.

**Misc**
The Misc tab contains options governing updater logging. You can choose to log updater actions in a log file, and you can specify a maximum size for the file.

---

**See:**

**AV Updater** 233
**AntiVirus** 231
**Content Filter and SecurityPlus** 210

## 5.2 Outbreak Protection

Outbreak Protection (OP) is a revolutionary real time anti-spam, anti-virus, and anti-phishing technology capable of proactively protecting an MDaemon email infrastructure automatically and within minutes of an outbreak. Included in SecurityPlus for MDaemon, Outbreak Protection requires SecurityPlus for MDaemon 3.0 or later and MDaemon PRO 9.5 or later, and it is accessible from MDaemon's Security menu (Security » Outbreak protection..., or Ctrl+Shift+1).

Outbreak Protection is completely content agnostic, meaning that it doesn't rely on strict lexical analysis of message content. Thus, it doesn't require heuristic rules, content filtering, or signature updates. Further, that means it is not fooled by the addition of seed text, clever spelling changes, social engineering tactics, language barriers, or differences in encoding techniques. Instead, OP relies on the mathematical analysis of message structure and message distribution characteristics over SMTP—it analyzes "patterns" associated with an email transmission and compares them to similar patterns collected from millions of email messages worldwide, which are sampled and compared in real time.

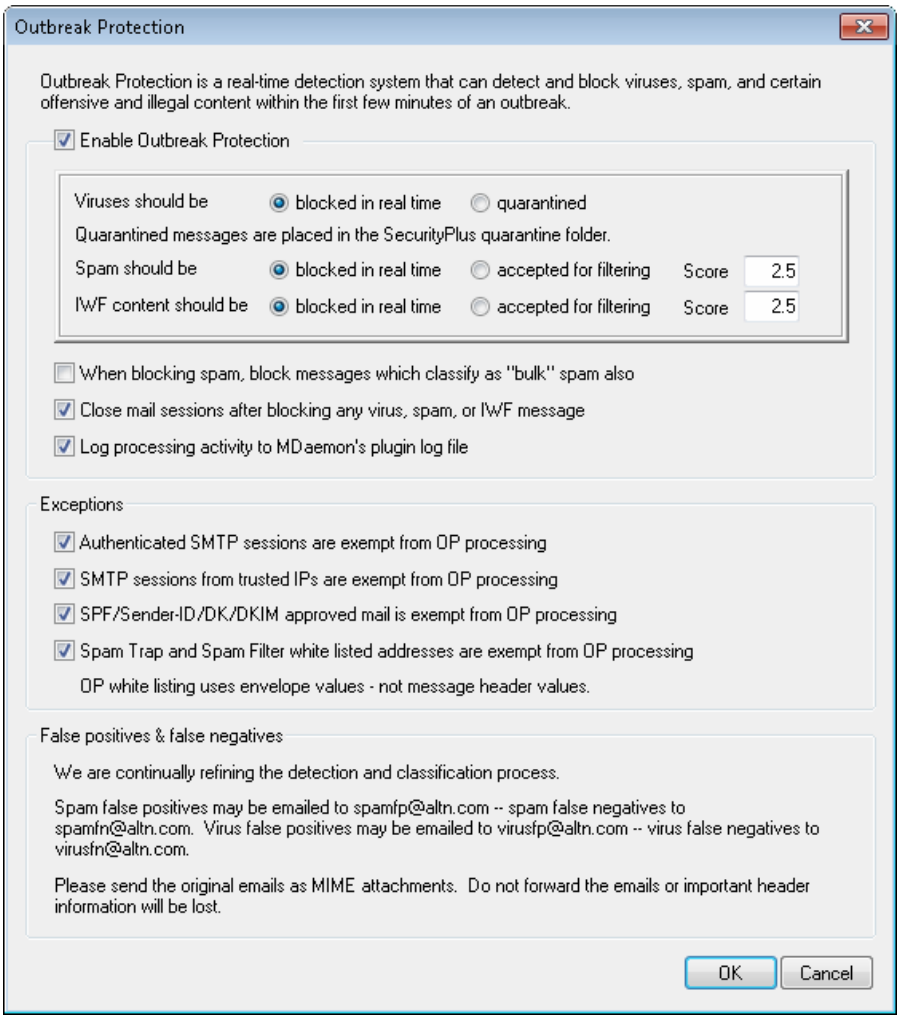
Because messages are being analyzed worldwide in real time, protection is provided within minutes—often seconds—of a new outbreak. For viruses, this level of protection is critical since it is often hours after an outbreak before a traditional antivirus vendor can verify and submit a virus signature update, and it can then be even longer before that update is put into production use. During that interval, servers without Outbreak Protection are vulnerable to that particular outbreak. Similarly, for spam messages it will often take time and effort to analyze the spam and create a safe filtering rule before it will be recognized by traditional heuristic and content based systems.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

It is important to note, however, that the Outbreak Protection feature in SecurityPlus is not a replacement for traditional anti-virus, anti-spam, and anti-phishing techniques. In fact, OP provides another specialized layer of protection on top of the existing heuristics, signature, and content based tools found within SecurityPlus and MDaemon. Specifically, OP is designed to deal with large-scale outbreaks rather than old, unique, or specifically targeted messages that can be more readily caught by the traditional tools.

Outbreak Protection is based on CommTouch RPD and Zero-Hour technology. It works by extracting patterns from your incoming mail and comparing them to patterns taken from millions of internet email messages sampled daily from numerous sources all over the world. In no way is the actual content of any message ever transmitted, nor can the message content ever be derived from the extracted patterns.

For more on SecurityPlus and Outbreak Protection, see the remainder of this section and visit: www.altn.com.




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## Outbreak Protection

**Enable Outbreak Protection**
Click this checkbox to enable Outbreak Protection for your server. Incoming messages will be analyzed to see if they are part of an ongoing virus, spam, or phishing outbreak. The remaining options on this dialog are used to determine what will be done with messages found to be part of an outbreak, and to designate the senders that will be exempt from OP processing.

**Viruses should be...**

**blocked in real time**
Select this option if you wish to block messages during the SMTP process when they are determined to be part of a virus outbreak. These messages will not be quarantined or delivered to their intended recipients—they will be rejected by the server.

**quarantined**
Select this option if you wish to accept messages that OP determines are part of a virus outbreak. Although these messages will not be rejected by the server, they will be quarantined instead of delivered to their intended recipients. Quarantined messages are placed in SecurityPlus' quarantine folder.

**Spam should be...**

**blocked in real time**
Select this option if you wish to block messages during the SMTP process when OP confirms that they are part of a spam outbreak. These messages will not be flagged as spam and delivered to their intended recipients—they will be rejected by the server. Messages classified by OP as "bulk" mail will not be blocked by this option unless you activate the *When blocking spam, block messages which classify as "bulk" spam also* option below. Messages classified as "bulk" by OP could simply be a part of certain very large mailing lists or other similar widely distributed content, so you may or may not consider those types of messages to be spam. For that reason, those types of messages generally shouldn't be scored negatively or blocked by OP.

**accepted for filtering**
Select this option if you wish to accept messages that OP confirms to be part of a spam outbreak, so that they can then be subjected to spam filtering and content filter processing. These messages will not be blocked by OP, but they will have their Spam Filter scores adjusted according to the *Score* option below.

When using the *accepted for filtering* option, OP will not directly cause a confirmed spam message to be blocked, but a message may still be blocked by MDaemon during the SMTP process if you have configured the Spam Filter to use the *SMTP rejects messages with scores greater than or equal to [xx]* option, located on the Spam Filter 242 screen.

For example, if the scoring option below caused a message's

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

> Spam Filter score to be 15.0, then the message would still be rejected as spam if you had also configured the Spam Filter's "*SMTP rejects...*" option to reject messages that have a score of 15.0 or greater.

**Score**
When using the *accepted for filtering* option above, this amount will be added to a message's Spam Filter score when OP confirms that the message is part of a spam outbreak.

## IWF Content

The following option applies to content identified by the Internet Watch Foundation (IWF) as referring to child abuse image sites (i.e. child pornography sites). It enables OP to use an integrated URL list provided by the IWF to detect and tag messages that refer to that content. The IWF operates an independent internet "hotline" for reporting potentially illegal online content, including child abuse content hosted anywhere in the world. They work in partnership with the police, governments, the wider online industry and the public to combat the availability of illegal online content. The Foundation's URL list is updated daily with new sites hosting child abuse images.

Many organizations have internal compliance rules governing the content of email sent or received by its employees, especially with regard to obscene or illegal material. In addition, many countries have outlawed the sending or receipt of such content. This feature can assist in your efforts to ensure compliance.

For more on the IWF, see:

http://www.iwf.org.uk/

**IWF content should be...**

**blocked in real time**
Choose this option if you wish to reject incoming messages during the SMTP process when they have IWF restricted content.

**accepted for filtering**
Choose this option if you wish to increase a message's Spam Filter score instead of rejecting it when it has IWF restricted content. The Spam Filter score will be increased by the amount specified in the *Score* option below.

**Score**
When the *accepted for filtering* option above is selected, this is the amount that will be added to a message's Spam Filter score when it contains IWF restricted content.

**When blocking spam, block messages which classify as "bulk" spam also**
Sometimes OP will identify certain messages that could be considered spam but aren't being sent from a known spammer or bot-net—as is sometimes the case with legitimate bulk mailings and newsletters. OP classifies these types of messages as "

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*Spam (bulk)*" rather than *"Spam (confirmed)*." Click this checkbox if you wish to apply OP's spam blocking features to "*Spam (bulk)*" mail as well. If this option is disabled, only messages classified as "*Spam (confirmed)*" will be affected by OP's spam blocking features above. Accepting this type of spam for later processing may be necessary for sites that want to receive bulk mailings but for some reason cannot white list the source or recipient.

**Log processing activity to MDaemon's plugin log file**
Enable this checkbox if you wish to log all OP processing activity into MDaemon's plugin log file.

## Exceptions

**Authenticated SMTP sessions are exempt from OP processing**
When this option is enabled, authenticated SMTP sessions are exempt from OP processing. This means that messages sent during that session will not be subjected to Outbreak Protection checks.

**SMTP sessions from trusted IPs are exempt from OP processing**
Enable this option if you wish to exempt trusted IP addresses from Outbreak Protection—messages arriving from a server at a trusted IP address not be subjected to OP checks.

**SPF/Sender-ID/DK/DKIM approved mail is exempt from OP processing**
Click this checkbox if you wish to exempt a message from OP processing when the sending domain appears on the Approved List[298] and it is validated by SPF, Sender-ID, DK, or DKIM.

**Spam Trap and Spam Filter white listed addresses are exempt from OP processing**
Click this option if you wish to exempt the Spam Honeypots[270] and Spam Filter white lists from Outbreak Protection. The "White List" applies to the recipient, or RCPT value given during the SMTP session. The "White List (from)" applies to the sender, or MAIL value given during the SMTP session. These operations are not based on message header values.

## False Positives and False Negatives

False positives, or classifying a legitimate message improperly as part of an outbreak, should rarely if ever happen. Should a false positive occur, however, you can send that message to us at **spamfp@altn.com** for spam/phishing false positives or **virusfp@altn.com** for virus false positives, so that we can use it to help refine and improve our detection and classification processes.

False negatives, or classifying a message as not part of an outbreak even though it is still spam or an attack, will happen more often than false positives. However, it worth noting that OP is not designed to catch all spam, virus attacks, and the like—it is simply one layer of protection that specifically targets outbreaks. Old messages, specifically targeted messages and the like, which are not part of a currently ongoing outbreak, might pass the OP check. Those sorts of messages should then be caught by the other SecurityPlus and MDaemon features further down the processing chain. Should a false negative occur, however, you can send that message to us at **spamfn@altn.com** for spam/phishing false negatives or

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**virusfn@altn.com** for virus false negatives, so that we can use it to help refine and improve our detection and classification processes.

When sending improperly classified messages to us, the original email should be sent as a MIME email attachment rather than forwarded. Otherwise, headers and other information critical to the classification process will be lost.

## 5.3 Spam Filter

### 5.3.1 Spam Filter

The Spam Filter is one of the main features in MDaemon's extensive suite of spam prevention tools. It incorporates heuristics to examine incoming email messages in order to compute a "score" based on a complex system of rules. The score is then used to determine the likelihood of a message being spam, and certain actions can be taken based on that score — you can refuse the message, flag it as possible spam, and so on.

Addresses can be white or black listed, or designated as completely exempt from Spam Filter examination. You can have a spam report inserted into messages, showing their spam scores and how those scores were achieved, or you can generate the report as a separate email and have the original spam message included with it as an attachment. Further, you can even use Bayesian 245 learning to help the Spam Filter learn to identify spam more accurately over time, thus increasing its reliability.

Finally, by examining many thousands of known spam messages, the rules have been optimized over time and are very reliable in detecting the fingerprint of a spam message. You can, however, customize or add new rules by editing the Spam Filter's configuration files to meet your specific needs.

MDaemon's Spam Filter uses an integrated, popular open-source heuristic technology. The homepage for the open-source project is:

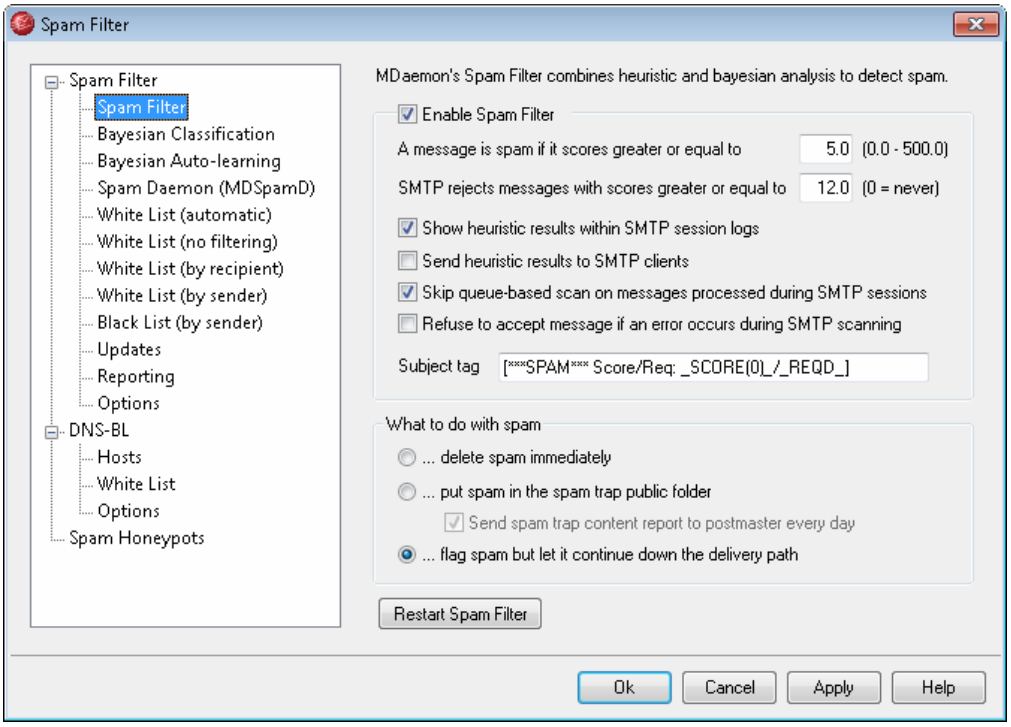
```
http://www.spamassassin.org
```

**See:**

**Spam Filter** 242
**DNS Black Lists** 264

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.1.1 Spam Filter




**Enable Spam Filter**

Check this box to activate the heuristic message-scoring, spam filtering system. None of the other Spam Filter options on this screen will be available until this option is enabled.

**A message is spam if its score is greater or equal to [XX] (0.0-500.0)**
The value that you specify here is the required spam threshold that MDaemon will compare to each message's spam score. Any message with a spam score greater than or equal to this amount will be considered spam, and then the appropriate actions will be taken based on your other Spam Filter settings.

**SMTP rejects messages with scores greater or equal to XX (0=never)**
Use this option to designate a spam score rejection threshold. When a message's spam score is greater than or equal to this score it will be rejected completely rather than proceed through the rest of the options and possibly be delivered. The value of this option should always be greater than the value of the "*A message is spam if its score...*" option above. Otherwise, a message would never be considered spam and have the rest of the Spam Filter's options applied to it—it would simply be rejected during delivery. Use "0" in this option if wish to disable scanning during the SMTP process, and if you do not want MDaemon to reject any messages regardless of their scores. If SMTP scanning is disabled then a queue-based scan will still be performed on the messages after they are accepted. The default setting for this option is "12.0".

Example,

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

If you have the spam score threshold set to 5.0 and the rejection threshold set to 10.0, then any message with a spam score that is greater than or equal to 5.0 but less than 10.0 will be considered spam and handled according to the rest of your Spam Filter settings. Any message with a spam score greater than or equal to 10.0 will be rejected by MDaemon during the delivery process.

You should monitor the spam filter's performance over time and refine both the spam and rejection thresholds to suit your need. For most people, however, a spam score threshold of 5.0 will catch most spam, with relatively few false negatives (spam that slips through unrecognized) and rarely any false positives (messages flagged as spam that are not). A rejection threshold of 10-15 will cause only messages that are almost certainly spam to be rejected. It is extremely rare that a legitimate message will have a score that high. The default rejection threshold is 12.

**Show heuristic results within SMTP session logs**
Click this option to log the results of heuristic processing during SMTP sessions to the SMTP session logs[104].

**Send heuristic results to SMTP clients**
Click this option to display heuristic processing results inline with SMTP session transcripts. This option is not available when you have your Spam Score rejection threshold set to "0", meaning that spam will never be rejected because of its score. For more information see, "*SMTP rejects messages with scores greater or equal to XX (0=never)*" above.

**Skip queue-based scan on messages processed during SMTP sessions**
By default, MDaemon scans messages during the SMTP session to determine whether or not they should be rejected for having a spam score above the rejection threshold. For messages that are accepted MDaemon will then perform another, queue-based, scan and treat the messages accordingly, based on their scores and your spam filter configuration. Click this option if you want MDaemon to omit the queue-based scan and treat the results of the initial Spam Filter scan as definitive. This can potentially significantly decrease CPU usage and increase the efficiency of the AntiSpam system. However, only the default SpamAssassin headers will be added to messages when the queue-based scan is omitted. If you have made any changes to the default SpamAssassin headers or specified custom headers in your `local.cf` file, those changes and additions will be ignored.

**Refuse to accept message if an error occurs during SMTP scanning**
Click this option if you want a message to be refused when an error is encountered while it is being scanned during the SMTP process.

**Subject tag**
This tag will be inserted at the beginning of the Subject header of all messages that meet or exceed the required spam score threshold. It can contain information about the spam score, and you can use your IMAP message filters to search for it and filter the message accordingly (assuming that you have the Spam Filter configured

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

to continue delivering spam messages). This is a simple method for automatically routing spam messages to a designated "spam" folder. If you want to dynamically insert the message's spam score and the value of the required spam threshold then use the tag "_HITS_" for the message's score and "_REQD_" for the required threshold. Alternatively, you can use "_SCORE(0)_" instead of "_HITS_"— this will insert a leading zero into lower scores, which can help ensure the proper sort-order when sorting messages by subject in some email clients.

Example,

A subject tag set to: `***SPAM*** Score/Req: _HITS_/_REQD_ -`
will cause a spam message with a score of 6.2 and the subject: "Hey, here's some spam!" to be changed to "***SPAM*** Score/Req: 6.2/5.0 – Hey, here's some spam!"

If "_SCORE(0)_" is substituted for "_HITS_" then it would be changed to "***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"

If you do not wish to alter the subject header then leave this option blank. No subject tag will be inserted.

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. The Subject tag configuration will be determined by the other server's settings. See: Spam Daemon 251, for more information.

### What to do with spam...

The Spam Filter will perform the action chosen below if a message's spam score is greater than or equal to the spam score specified above.

**...delete spam immediately**
Choose this option if you wish simply to delete any incoming message whose spam score is equal to or exceeds the designated limit.

**...put spam in the spam trap public folder**
Choose this option if you want to flag messages as spam and then move them to the spam public folder rather than allow them to be delivered.

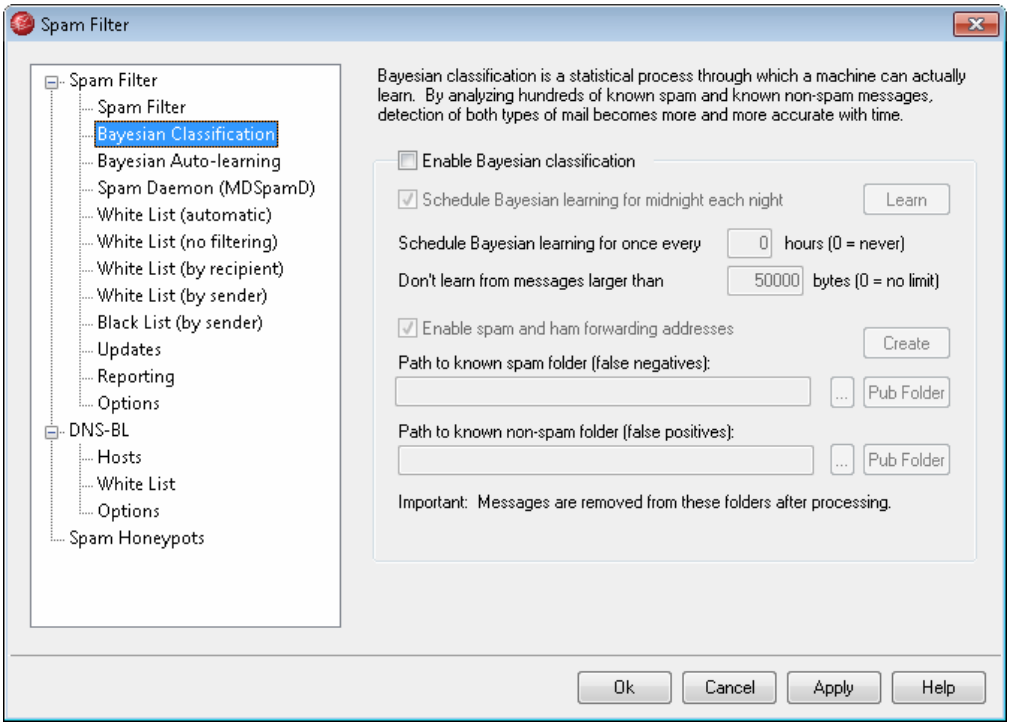
**Send spam trap content report to postmaster every day**
When using the *...put spam in the spam trap public folder* option above, check this box if you would like the postmaster to receive a daily message with a summary of the folder's contents.

**...flag spam but let it continue down the delivery path**
Choose this option if you want to go ahead and deliver each spam message to its intended recipient, but flag it as spam by inserting various spam headers and/or tags designated above and on the Reporting 261 screen. This is the default

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

option, which allows users to take advantage of options such as filtering mail into a spam folder for their review and thus avoid losing messages that may be erroneously labeled as spam (i.e. false positives).

### 5.3.1.2 Bayesian Classification




Bayesian Classification is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 251 screen for more information.

The Spam Filter supports Bayesian learning, which is a statistical process that can optionally be used to analyze spam and non-spam messages in order to increase the reliability of spam recognition over time. You can designate a folder for spam messages and non-spam message that will can be scanned manually or automatically at regular intervals. All of the messages in those folders will be analyzed and indexed so that new messages can be compared to them statistically in order to determine the likelihood that they are spam. The Spam Filter can then increase or decrease a message's spam score based upon the results of its Bayesian comparison.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

The Spam Filter will not apply a Bayesian classification to messages until a Bayesian analysis has been performed on the number of spam and non-spam messages designated on the Bayesian Auto-learning[249] screen. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

## Bayesian Classification

**Enable Bayesian classification**
Click this check box if you want each message's spam score to be adjusted based on a comparison to the currently known Bayesian statistics.

**Schedule Bayesian learning for midnight each night**
When this option is active, once each day at midnight the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you wish to schedule Bayesian learning for some other time interval then clear this option and use the *Schedule Bayesian learning for once every XX hours* option below. If you do not wish Bayesian learning to ever occur automatically, then clear this option and specify "0" hours in the option below.

**Schedule Bayesian learning for once every XX hours (0=never)**
If you wish Bayesian learning to occur at some time interval other than once each night at midnight, then clear the above option and specify a number of hours in this option instead. Each time that number of hours has elapsed, the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you do not wish Bayesian learning to ever occur automatically, then clear the above option and specify "0" hours in this option.

If for some reason you do not want the messages to be deleted after they are analyzed then you can prevent that by copying `LEARN.BAT` to `MYLEARN.BAT` in the `\MDaemon\App\` subfolder and then deleting the two lines that begin with "`if exist`" near the bottom in that file. When the `MYLEARN.BAT` file is present in that folder MDaemon will use it instead of `LEARN.BAT`. See `SA-Learn.txt` in your `\MDaemon\SpamAssassin\` subfolder for more information.

For more detailed information on heuristic spam filtering technology and Bayesian learning, visit:

http://www.spamassassin.org/doc/sa-learn.html

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Don't learn from messages larger than XX bytes (0=no limit)**
Use this option to designate a maximum message size for Bayesian analysis. Messages larger this value will not be analyzed. Specify "0" in this option if you do not wish to implement any size restriction.

**Learn**
Click this button to initiate a manual Bayesian analysis of the designated folders rather than waiting for the automatic analysis.

**Enable spam and ham forwarding addresses**
Click this check box if you wish to allow users to forward spam and non-spam (ham) messages to designated addresses so that the Bayesian system can learn from them. The default addresses that MDaemon will use are "SpamLearn@<domain>" and "HamLearn@<domain>". Messages sent to these addresses must be received via SMTP from a session that is authenticated using SMTP AUTH. Further, MDaemon expects the messages to be forwarded to the above addresses as attachments of type "message/rfc822". Any message of another type that is sent to these email addresses will not be processed.

You can change the addresses MDaemon uses by adding the following key to the CFilter.INI file:

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

**Note:** the last character of these values must be "@".

**Create**
Click this button to create spam and non-spam Public IMAP Folders 74 automatically, and to configure MDaemon to use them. The following folders will be created:

| | |
|---|---|
| \Bayesian Learning.IMAP\ | Root IMAP folder |
| \Bayesian Learning.IMAP\Spam.IMAP\ | This folder is for false negatives (spam that doesn't score high enough to get flagged as such). |
| \Bayesian Learning.IMAP\Non-Spam.IMAP\ | This folder is for false positives (non-spam messages that erroneously score high enough to get flagged as spam). |

By default, access permission to these folders is only granted to local users of local domains and is limited to Lookup and Insert. The postmaster's default permissions are Lookup, Read, Insert, and Delete.

**Path to known spam folder (false negatives):**
This is the path to the folder that will be used for Bayesian analysis of known spam messages. Only copy messages to this folder which you consider to be spam. You should not automate the process of copying messages to this folder unless doing so

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

via the Bayesian Auto-learning 249 or Spam Honeypots 270 options. Automating this process by some other means could potentially cause non-spam messages to be analyzed as spam, which would decrease the reliability of the Bayesian statistics.

**Path to known non-spam folder (false positives):**
This is the path to the folder that will be used for Bayesian analysis of messages that are definitely **not** spam. Only messages that you do **not** consider to be spam should be copied to this folder. You should not automate the process of copying messages to this folder unless doing so via the Bayesian Auto-learning 249 options. Automating this process by some other means could potentially cause spam messages to be analyzed as non-spam, which would decrease the reliability of the Bayesian statistics.

**Pub Folder**
Click one of these buttons to designate one of your existing Public Folders as the Bayesian directory. This is an easy way for your users to place their messages incorrectly categorized as spam or non-spam into your Bayesian directories for analysis. Note, however, that giving access to more people increases the likelihood that some messages will be put into the wrong folders thus skewing the statistics and decreasing reliability.

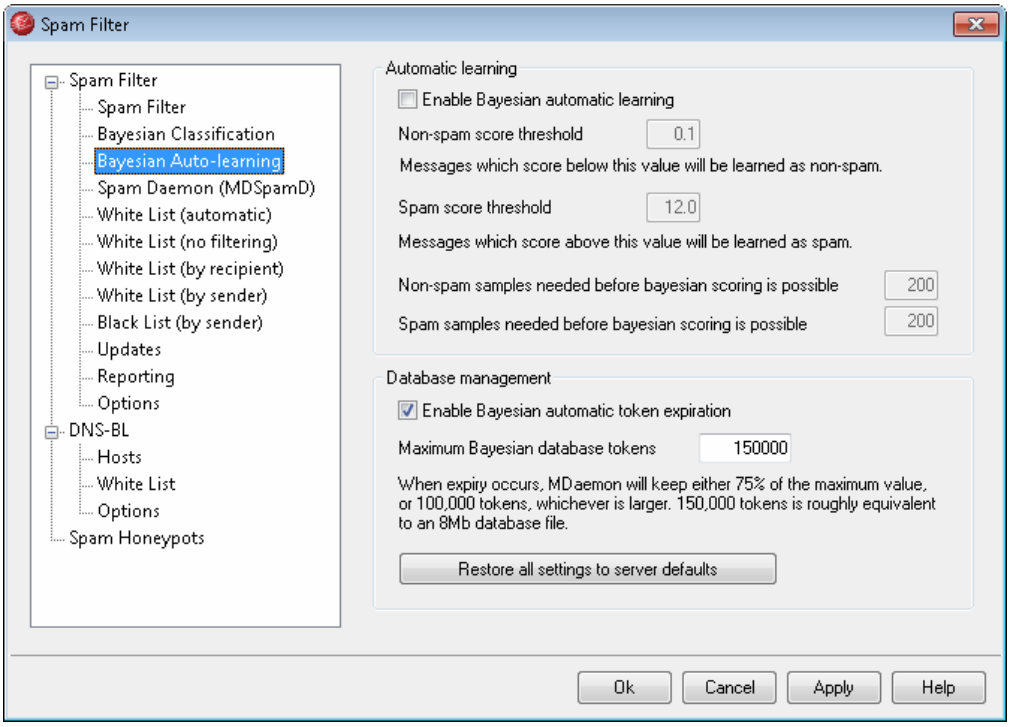
If you rename a Public folder via a mail client, Windows Explorer, or some other means, then you must manually reset this path to the appropriate new folder name. If you rename a folder but do not change its path here, the Spam Filter will continue to use this path for the Bayesian folder instead of the new one.

**See:**

**Bayesian Auto-learning** 249
**Spam Honeypots** 270

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.1.3 Bayesian Auto-learning



Bayesian Auto-learning is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 251 screen for more information.

#### Automatic Learning

**Enable Bayesian automatic learning**
With automatic Bayesian learning you can designate spam and non-spam scoring thresholds, which make it possible for the Bayesian learning system to learn from messages automatically rather than requiring you to manually place those messages in the spam and non-spam folders. Any message scoring below the non-spam threshold will be treated by automatic learning as non-spam, and any message scoring above the spam threshold will be treated as spam. With automatic learning, old expired tokens that are removed from the database (see *Database Management* below) can be replaced automatically. This prevents the need for manual retraining to recover expired tokens. Automatic Learning can be useful and beneficial as long if you are careful in setting your thresholds, to avoid placing improperly classified messages in the folders.

**Non-spam score threshold**
Messages with a spam score below this value will be treated as non-spam messages

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

by the Bayesian Classification system.

**Spam score threshold**
Messages with a spam score above this value will be treated as spam messages by the Bayesian Classification system.

**Non-spam samples needed before Bayesian scoring is possible**
The Spam Filter will not apply a Bayesian classification to messages until this number of non-spam messages (and spam messages specified in the next option) has been analyzed by the Bayesian system. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

**Spam samples needed before Bayesian scoring is possible**
Just as the previous option applies to non-spam messages, this option is for designating the number of *spam* messages that must be analyzed before the Spam Filter will begin applying a Bayesian classification to messages.

### Database Management

**Enable Bayesian automatic token expiration**
Click this option if you want the Bayesian system to automatically expire database tokens whenever the number of tokens specified below is reached. Setting a token limit can prevent your Bayesian database from getting excessively large.

**Maximum Bayesian database tokens**
This is the maximum number of Bayesian database tokens allowed. When this number of tokens is reached, the Bayesian system removes the oldest, reducing the number to 75% of this value, or to 100,000 tokens, whichever is higher. The number of tokens will never fall below the larger of those two values regardless of how many tokens are expired. Note: 150,000 database tokens is approximately 8Mb.

**Restore all settings to server defaults**
Click this button to restore all of the Bayesian advanced options to their default values.

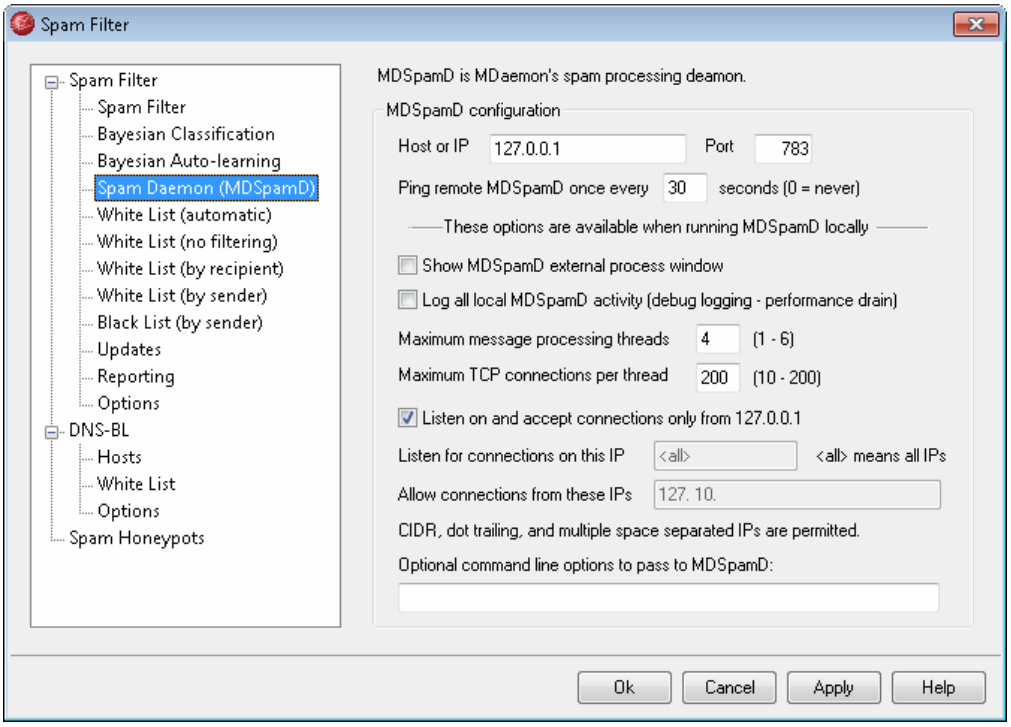
---

**See:**

**Bayesian Classification** 245
**Spam Honeypots** 270

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.3.1.4 Spam Daemon (MDSpamD)




MDaemon's spam filtering system runs as a separate daemon—the MDaemon Spam Daemon (MDSpamD), which is fed messages via TCP/IP for scanning. This greatly increases the Spam Filter's performance and makes it possible for you to run MDSpamD locally, on a separate computer, or have MDaemon use another MDSpamD (or any other Spam Daemon enabled product) running at some other location. By default MDSpamD runs locally and receives messages on port 783 at 127.0.0.1, but you can configure a different port and IP address if wish to send the messages to some other spam daemon running at a different location or on a different port.

#### MDSpamD Configuration

**Host or IP**
This is the host or IP address to which MDaemon will send messages to be scanned by MDSpamD. Use `127.0.0.1` if MDSpamD is running locally.

**Port**
This is the port on which the messages will be sent. The default MDSpamD port is 783.

**Ping remote MDSpamD once every XX seconds (0=never)**
If you are using a spam daemon that is running at a remote location, you can use this option to ping its location periodically. Use "0" if you do not wish to ping that location.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### These options are available when running MDSpamD locally

**Show MDSpamD external process window**
When MDSpamD is running locally, enable this option if you would like it to run in an external process window. This option will cause the output from MDSpamD to be piped to the external process window rather than to MDaemon's internal UI or logging system. Using this option could increase performance since MDSpamD's data will not have to be piped into and logged by MDaemon. However, no log file will be created and as such this feature cannot be used with the logging option below, nor will MDSpamD data appear in the *Security»MDSpamD* tab of MDaemon's main GUI.

**Log all local MDSpamD activity (debug logging—performance drain)**
Click this option if you wish to log all MDSpamD activity. This option is unavailable if you are using the *Show MDSpamD external process window* option above. Further, if using user credentials on the Windows Service 205 dialog rather than running MDaemon under the SYSTEM account, no MDSpamD activity will be logged.

When using this logging option, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use this option for debugging purposes.

**Maximum message processing threads (1-6)**
This is the maximum number of threads that MDaemon will use for internal processing. You can set this value from 1 to 6.

**Maximum TCP connections per thread (10-200)**
This is the maximum number of TCP connections accepted by an MDSpamD thread before it branches into another thread. You can set this value from 10 to 200.

**Listen on and accept connections only from 127.0.0.1**
Click this option if do not you wish to allow your local MDSpamD to accept connections from any external source. Only connections from the same machine on which it is running will be allowed.

**Listen for connections on this IP**
If the previous option is disabled, you can use this option to bind or restrict connections to a specific IP address. Only connections to the designated IP address will be allowed. Use "<all>" if you do not wish to restrict MDSpamD to any particular IP address.

**Allow connections from these IPs**
These are the IP addresses from which MDSpamD will accept incoming connections. Connections from other IP addresses will be rejected. This is useful if you wish to allow connections from another server in order to share Spam Filter processing.

### Optional command line options to pass to MDSpamD:

MDSpamD can accept many command line options, documented at:

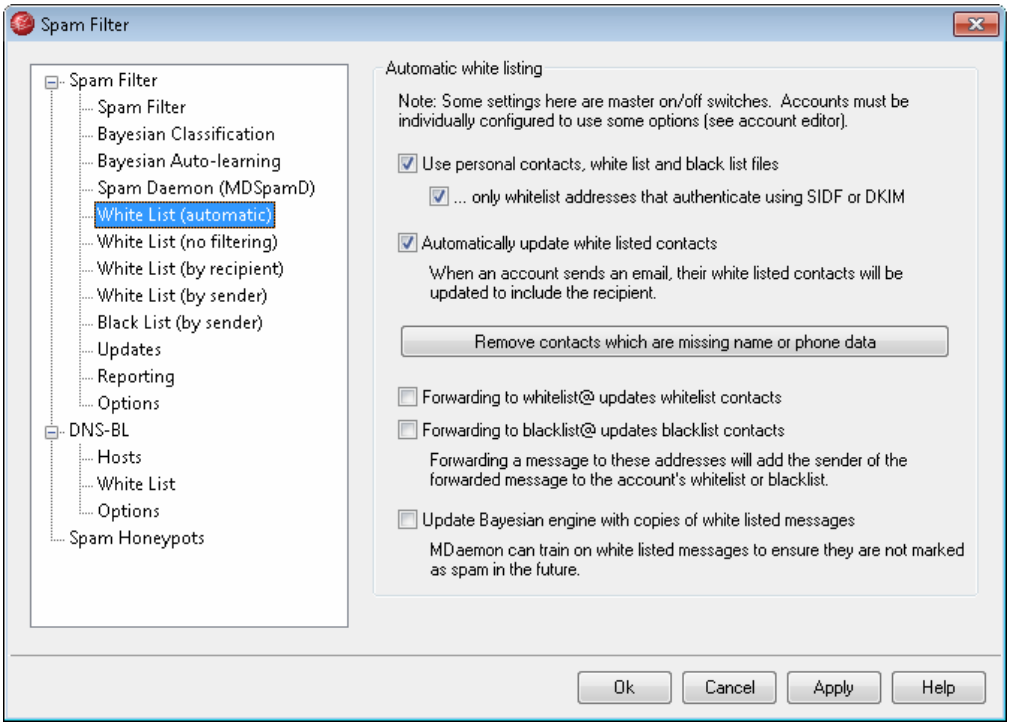
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

http://spamassassin.apache.org/

If you wish to use any of those options, construct a string containing the desired options and place it here.

Some of those options can be configured via the settings on this dialog and therefore do not need to be set up manually using command line options.

### 5.3.1.5 White List (automatic)




#### Automatic White Listing

**Use personal contacts, white list and black list files**
Click this option to allow each user's personal contacts, white list and black list files to be used as Spam Filter white and black lists. For each incoming message, MDaemon will search the recipient account's contacts, white list, and black list for the sender of the message. If the sender is found then the message will be white or black listed automatically. If you do not wish to apply automatic white and black listing to every MDaemon user then you can disable it for individual users by clearing the *Spam Filter uses personal contacts, white list, and black list files* option on the Options 377 screen of the Account Editor.

**Note:** Keeping your contacts updated and synchronized with WorldClient, the Windows Address Book, and other MAPI mail clients that use the Windows Address Book can be easily done using ComAgent 114.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...only whitelist addresses that authenticate using SIDF or DKIM**
When this option is enabled, MDaemon will not white list the message unless the sender was authenticated via the Sender ID Framework 282 (SIDF) or DomainKeys Identified Mail 284 (DKIM). This option helps to avoid white listing messages with spoofed addresses.

**Automatically update white listed contacts**
When this option is enabled, MDaemon will automatically add any non-local email addresses to which you send mail to your personal white list folder. When used in conjunction with "*Use personal contacts, white list and black list files*" above, the number of Spam Filter false positives can be drastically reduced.

If you do not wish to apply automatic white list updating to every MDaemon user then you can disable it for individual users by clearing the "*Update white listed contacts with mail recipients*" check box on the Options 377 screen of the Account Editor.

This option is disabled for accounts using autoresponders.

**Remove contacts which are missing name or phone data**
Click this button if you wish to remove every contact that contains only an email address from every user's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who have been using MDaemon's automatic white listing option prior to version 11 purge contacts that were added purely as a function of the white list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated white list folder. This could result in users having many entries in their contacts that they would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

**Forwarding to whitelist@ updates whitelist contacts**
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, white list, and black list files*" on the Account Editor's Options screen can forward messages to `whitelist@<domain>` and have MDaemon add the sender of the original message to the account's white list. The white listed address is taken from the forwarded message's `From` header.

Messages forwarded to `whitelist@<domain>` must be forwarded as attachments of the type `message/rfc822`, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

You can change the address MDaemon uses by editing the following key in the `CFILTER.INI` file:

```
[SpamFilter]
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

```
WhiteListAddress=MyWhiteListAddress@
```

**Note:** the last character must be "@".

**Forwarding to blacklist@ updates blacklist contacts**
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, white list, and black list files*" on the Account Editor's Options screen can forward messages to `blacklist@<domain>` and have MDaemon add the sender of the original message to the account's black list. The black listed address is taken from the forwarded message's `From` header.

Messages forwarded to `blacklist@<domain>` must be forwarded as attachments of the type `message/rfc822`, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

**Update Bayesian engine with copies of white listed messages**
Check this box to cause qualified messages to be copied automatically into the Bayesian non-spam learning folder (designated on the Bayesian 245 screen). This helps to automate the process of providing the Bayesian engine with samples of non-spam messages. Regularly providing the Bayesian engine with new examples of non-spam to learn from will increase its reliability over time and help to reduce the number of false positives (i.e. messages that are erroneously classified as spam).

To qualify for this feature, an incoming message must be addressed to a local user and the sender must be someone in his address book file. If the message is outgoing, then it must be the recipient who is in the address book. If you do not want any outgoing messages to qualify, then use Notepad to edit the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
UpdateHamFolderOutbound=No (default = Yes)
```

When a message qualifies, it is copied into the Bayesian non-spam learning folder even if Bayesian scheduled learning is disabled on the Bayesian screen. Thus, when scheduled learning is later enabled, or when learning is manually activated, a set of non-spam messages will be ready for analysis. Not every message that qualifies, however, is copied into the learning folder. When the feature is activated, MDaemon will copy qualified messages until a designated number is reached. Subsequently it will copy single messages at designated intervals. By default, the first 200 qualifying messages will be copied and then every tenth qualifying message after that. The initial number copied is equal to the number designated in the option, "*Non-spam samples needed before Bayesian scoring is possible*" located on the Bayesian Auto-learning 249 screen. Changing that setting will also change this value. If you wish to change the interval by which subsequent messages are copied, you can do so by editing the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
HamSkipCount=10 (default = 10)
```

Finally, once a designated total number of messages has been copied, the entire process will be begin again — 200 will be copied and then every tenth (or an alternate value if you have changed these settings). By default, the process will be

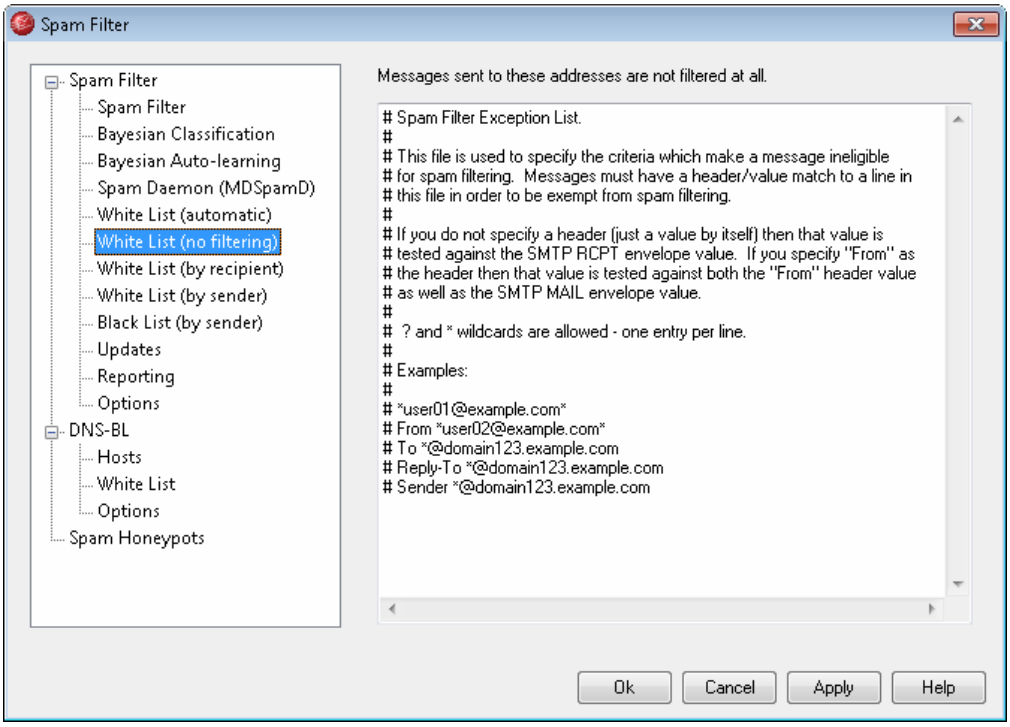
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

restarted after 500 qualifying messages have been copied. You can change this value by editing the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
HamMaxCount=500 (default = 500)
```

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning functions are determined by the other server's settings and are performed on the other server. See Spam Daemon 251 for more information.

### 5.3.1.6 White List (no filtering)



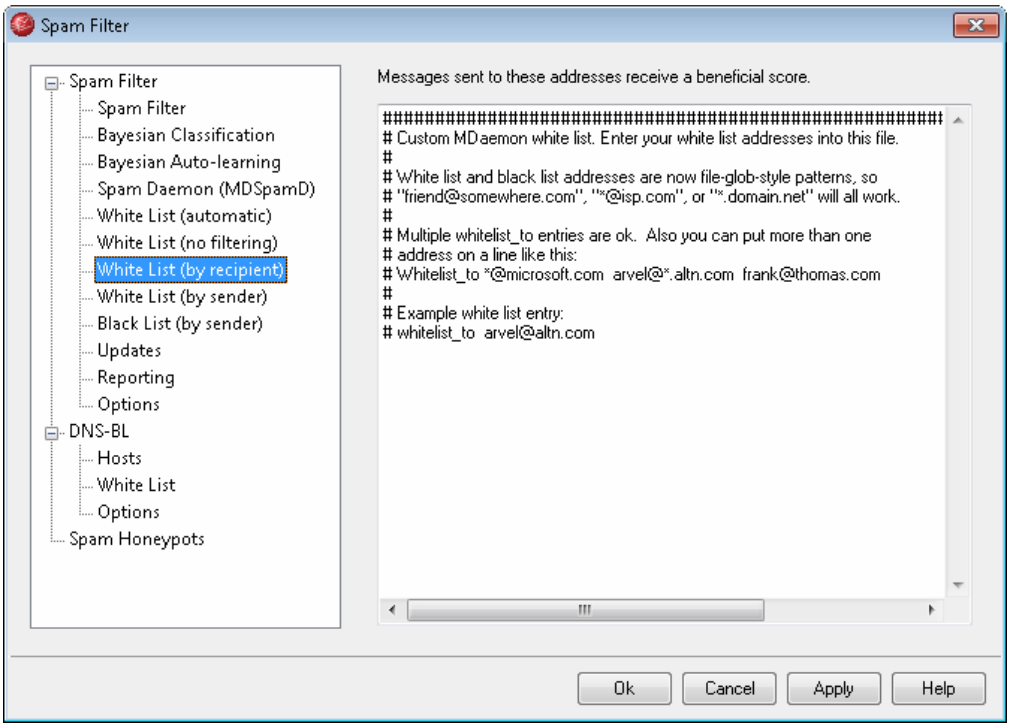

**Messages sent to these addresses are not filtered at all**
Use this screen to designate recipient addresses that you wish to be exempt from spam filtering. Messages destined for these addresses will not be processed through the spam filter.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 251 for more

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

information.

### 5.3.1.7 White List (by recipient)

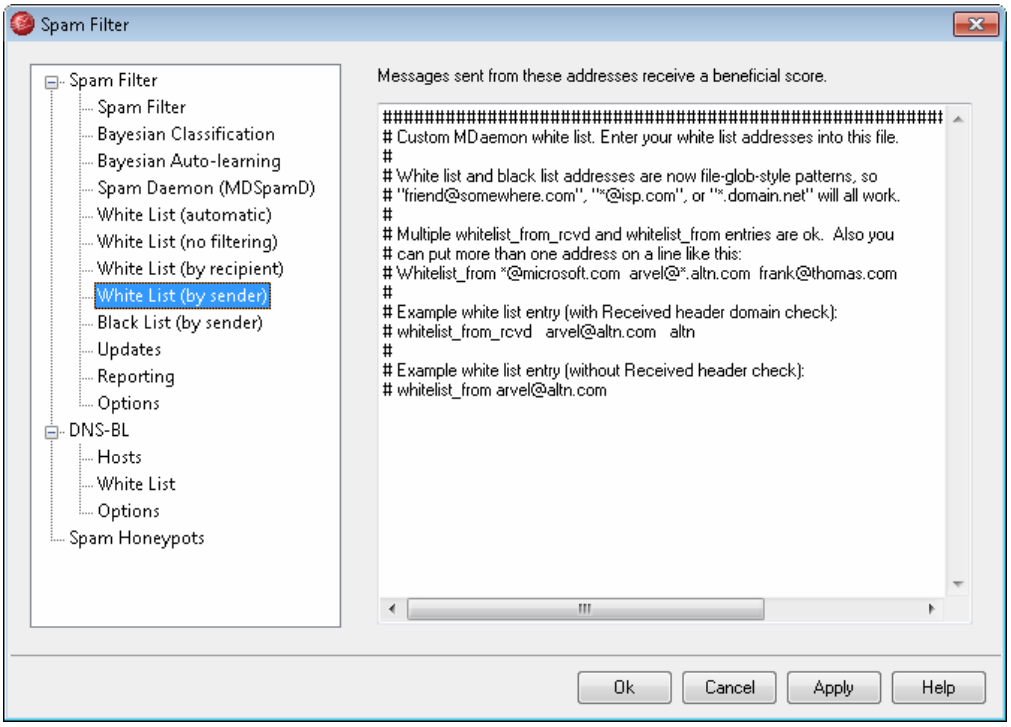



**Messages sent to these addresses receive a beneficial score**
Including an address on this white list does not automatically guarantee that a message to that address will not be considered spam. Instead, messages to the white listed addresses will have the amount specified on the Spam Filter 242 screen subtracted from their spam scores. For example, if you have the spam score threshold set to 5.0 and the white list value set to 50, and then a particularly excessive spam message arrives that gets a spam score of 55.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This would rarely happen, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 251 for more information.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.1.8 White List (by sender)

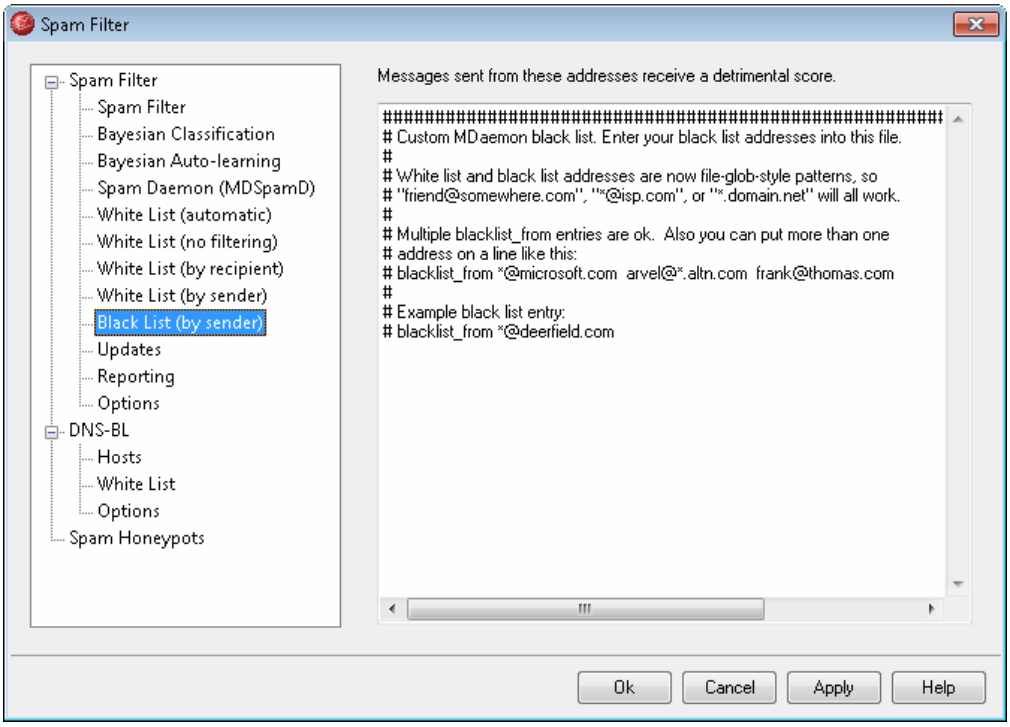



**Messages sent from these addresses receive a beneficial score**
Including an address on this white list does not automatically guarantee that a message from that address will not be considered spam. Instead, messages from these white listed addresses will have the amount specified on the Spam Filter[242] screen subtracted from their spam scores. For example, if you have the spam score threshold set to 5.0 and the white list value set to 50, and then a particularly excessive spam message arrives that gets a spam score of 55.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This would rarely happen, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon[251] for more information.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.1.9 Black List (by sender)

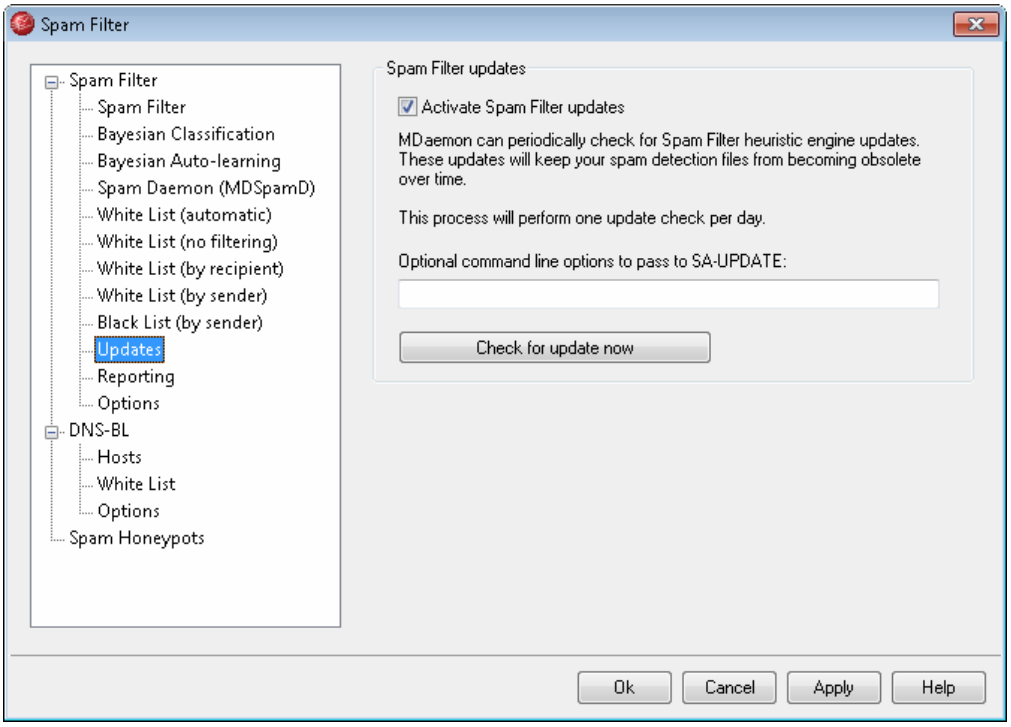



**Messages sent from these addresses receive a detrimental score**
Including an address on this black list does not automatically guarantee that a message from that address will be considered spam. Instead, messages from the black listed addresses will have the amount specified on the Spam Filter 242 screen added to their spam scores. For example, if you have the spam score threshold set to 5.0 and the black list value on the spam filter screen set to 50, and a particularly low-scoring message arrives that gets a spam score of -50.0 or lower before the black list value is added, then the final spam score of the message will be less than 5.0, thus denoting it as a legitimate non-spam message. This would rarely happen, however, because messages rarely have that much subtracted from their spam scores unless they contain some other special element, such as a white listed address.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 251 for more information.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.1.10 Updates



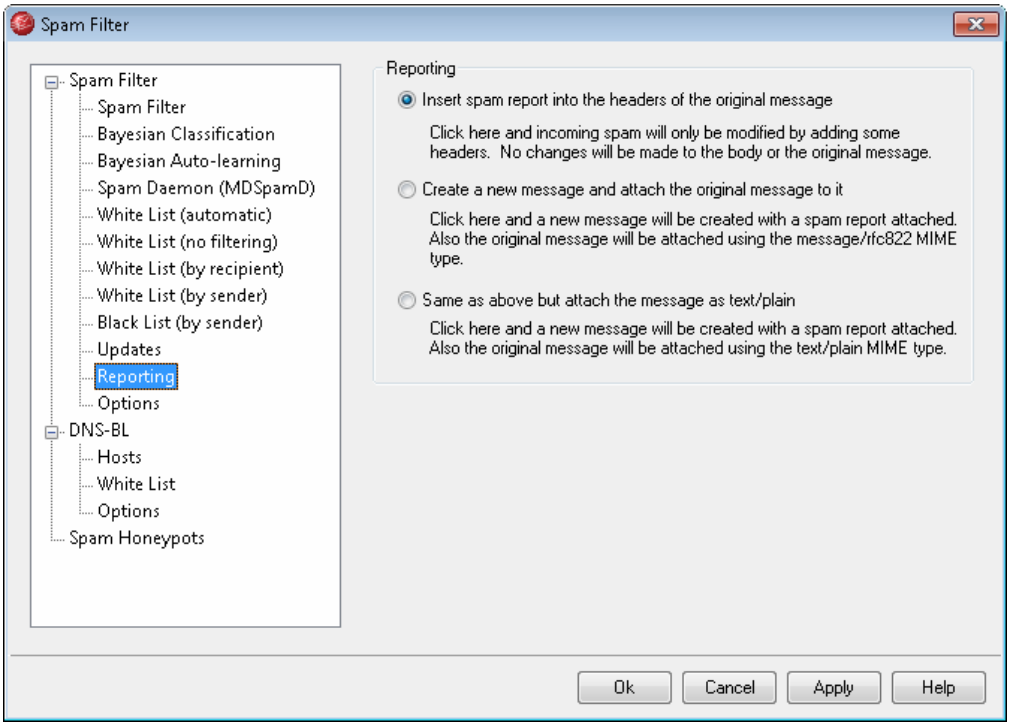

#### Spam Filter Updates

**Activate Spam Filter updates**
Click this check box if you want the Spam Filter be updated automatically. Once per day MDaemon will to see if there are any updates available for the Spam Filter heuristics engine, and if so it will download and install them automatically.

**Check for update now**
Click this button to check immediately for a Spam Filter rules update.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.3.1.11 Reporting




The Spam Filter Reporting options are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. Spam Filter Reporting will be controlled by the other server's settings. See the Spam Daemon 251 screen for more information.

#### Reporting

**Insert spam report into the headers of the original message**
This is the default reporting option. Use this option if you want the Spam Filter to insert a spam report into each spam message's headers. The following is an example of a simple spam report:

```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
  *  3.0 -- Message has been marked by MDaemon's DNS-BL
  *  2.9 -- BODY: Impotence cure
  *  2.2 -- BODY: Talks about exercise with an exclamation!
  *  0.5 -- BODY: Message is 80% to 90% HTML
  *  0.1 -- BODY: HTML included in message
  *  1.6 -- BODY: HTML message is a saved web page
  *  2.0 -- Date: is 96 hours or more before Received: date
```

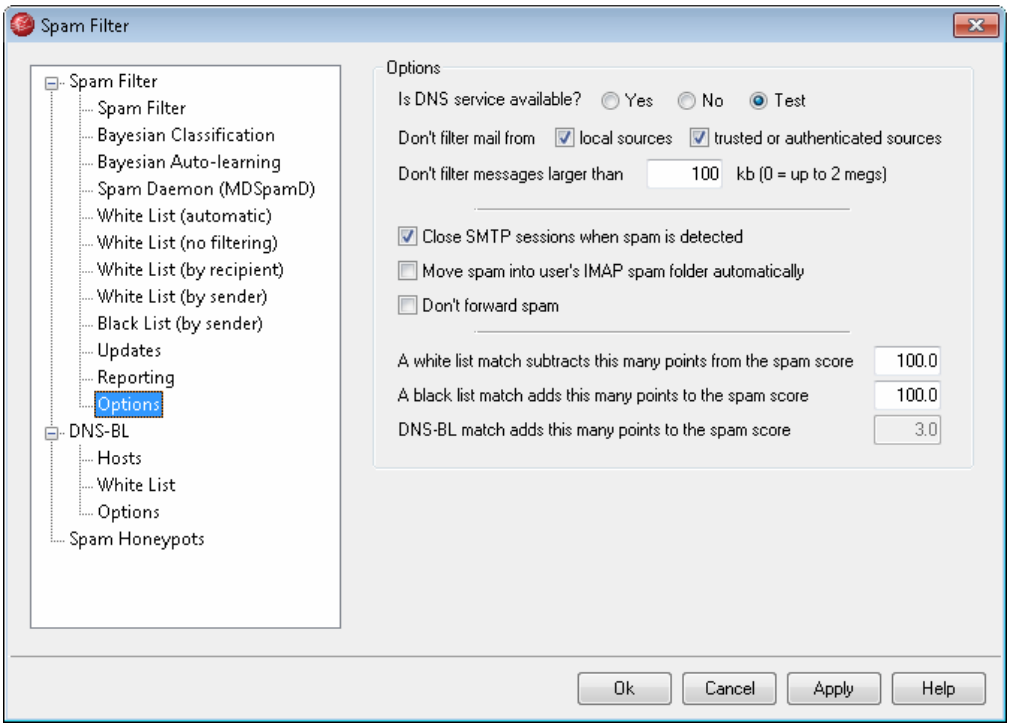
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

```
---- End of Spam Filter results
```

**Create a new message and attach the original message to it**
Choose this reporting option if you want spam to cause a new email message to be created containing the spam report. The original spam message will be included with it as a file attachment.

**Same as above but attach the message as text/plain**
Like the previous reporting option, this option will generate the spam report as a new message that includes the original spam message as a file attachment. The difference is that the original message will be attached using the text/plain MIME type. Because spam sometimes contains HTML code that is unique for each message and can potentially reveal to the spammer which email and IP address opened it, this method can prevent that from happening by converting the HTML code to plain text.

### 5.3.1.12 Options




**Is DNS service available?**
These options allow you to choose whether or not DNS is available to the Spam Filter when processing messages. You may choose one of the following options:

**Yes -** DNS is available. SURBL/RBL and other rules that require DNS connectivity will therefore be utilized.

**No -** DNS is not available. Spam filtering rules that require DNS will not be utilized.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Test -** DNS availability will be tested and if present it will be used. This is the default setting.

**Don't filter mail from...**

**local sources**
Click this check box if you want messages from local users and domains to be exempt from filtering.

**trusted or authenticated sources**
Enable this option if you want messages sent from trusted domains or authenticated senders to be exempt from spam filtering.

**Don't filter messages larger than [XX] kb (0=up to 2MB)**
It is typical for spam messages to be fairly small since the usual goal of the spammers is to deliver as many messages as possible in the shortest amount of time. If you want messages over a certain size to be exempt from spam filtering then specify the size (in KB) here. Use "0" if you want only very large messages to be exempt from spam filtering—only messages over 2MB will not be filtered.

**Close SMTP sessions when spam is detected**
This option is enabled by default and will close an SMTP session if an inline scan detects a spam message.

**Move spam into user's IMAP spam folder automatically**
Click this option and MDaemon will automatically place each message that the Spam Filter determines to be spam into each user's "Spam" IMAP folder (if such a folder exists). It will also automatically create the folder for each new user account that is added.

When you click this option you will also be asked whether or not you would like MDaemon to create this folder for each of your already existing user accounts. If you choose "Yes" then a folder will be created for all users. If you choose "No" then a folder will only be created when each new user is added. Any folders that already exist for some or all of your users will not be altered or affected in any way.

**Don't forward spam**
Click this check box if you do not wish to allow spam messages to be forwarded.

The remaining options on this screen are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. See the Spam Daemon 251 screen for more information.

**A white list match subtracts this many points from the spam score**
Placing an address on the Spam Filter's White List (by recipient) 257 or White List (by sender) 258 screens does not automatically guarantee that a message to or from that address will not be considered spam. Instead, those white listed addresses will

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

simply have the amount specified in this control subtracted from their spam scores. For example, if you have the spam score threshold set to 5.0 and this value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the white list value is subtracted, then the final spam score of the message will be at least 5.0 — thus denoting it as spam. This would rarely happen, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blacklisted address. Of course, if you set the white list subtraction value to a much lower amount then it would occur much more frequently.

If you wish to cause messages addressed to certain recipients to bypass the Spam Filter completely rather than simply adjust their scores, include those recipient addresses on the White List (no filtering) 256 screen. You can also exclude messages from Spam Filter scoring based on the sender by using the options on the White List (automatic) 253 screen.

**A black list match adds this many points to the spam score**
This value is added to the spam score of messages from addresses found on the Black List (by sender) 259 screen. As with the white list option above, including an address on the Spam Filter's black list doesn't guarantee that a message from that address will be considered spam. Instead, the value specified in this option will be added to the message's spam score, which will then be used to determine whether or not the message is spam.

**DNS-BL match adds this many points to the spam score**
If you are using DNS Black Lists 264 then you can use this option to specify a value that will be added to a message's spam score when a DNS-BL match is found. Sometimes the Spam Filter's heuristic examination of a message may not score it high enough to be considered spam, but a DNS-BL lookup may show that it probably is spam. Adding this value to the spam score of these messages can help to reduce the number of spam messages that manage to slip through undetected by the Spam Filter.

## 5.3.2 DNS Black Lists (DNS-BL)

DNS Black Lists (DNS-BL) can be used to help prevent spam email from reaching your users. This security feature allows you to specify several DNS blacklisting services (which maintain lists of servers known to relay spam) that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these services, the message(s) will be refused or flagged according to the settings on the Options 267 screen.

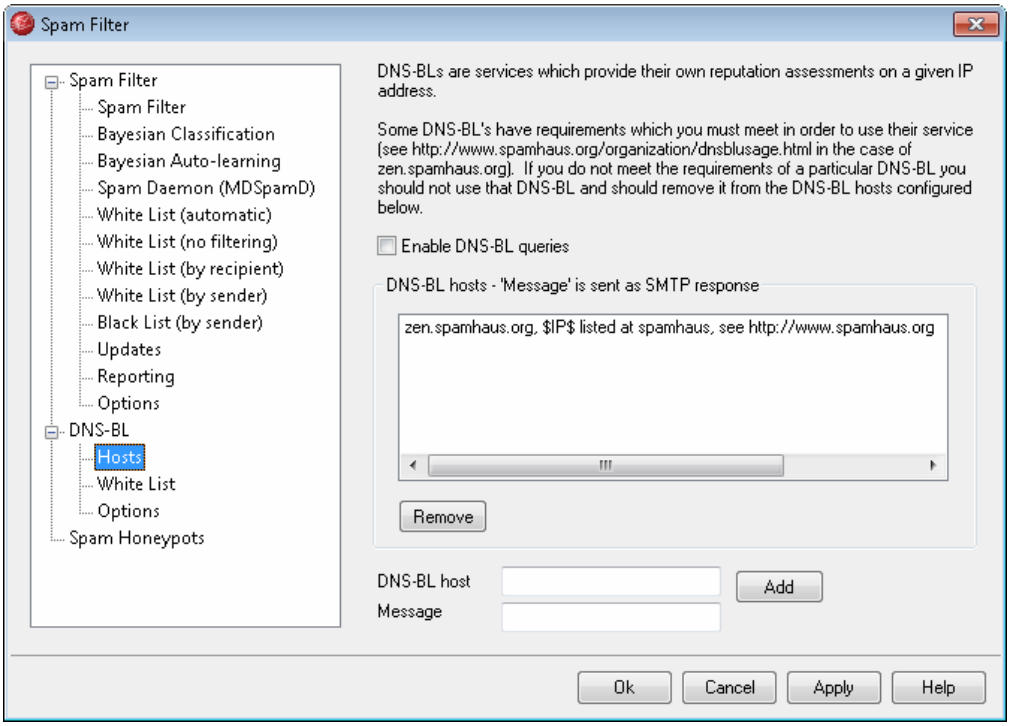
DNS Black Lists includes a White List for designating IP addresses that you wish to make exempt from DNS-BL queries. Before activating DNS-BL, you should make sure that your local IP address range is on the White List to prevent lookups on those addresses. "127.0.0.1" is exempt and therefore doesn't need to be added to the list.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**DNS-BL Hosts** 265
**DNS-BL Options** 267
**DNS-BL White List** 266

### 5.3.2.1 Hosts




#### DNS-BL Hosts

**Enable DNS-BL queries**
Activate this option if you wish to check incoming mail against DNS Black Lists. MDaemon will query each listed host when performing a DNS-BL lookup on the sending IP address. If a host replies to the query with a positive result, MDaemon can flag the message or refuse to accept it, depending on which options you have enabled on the DNS-BL Options 267 screen.

**Remove**
Select an entry from the DNS-BL service list and click this button to remove it from the list.

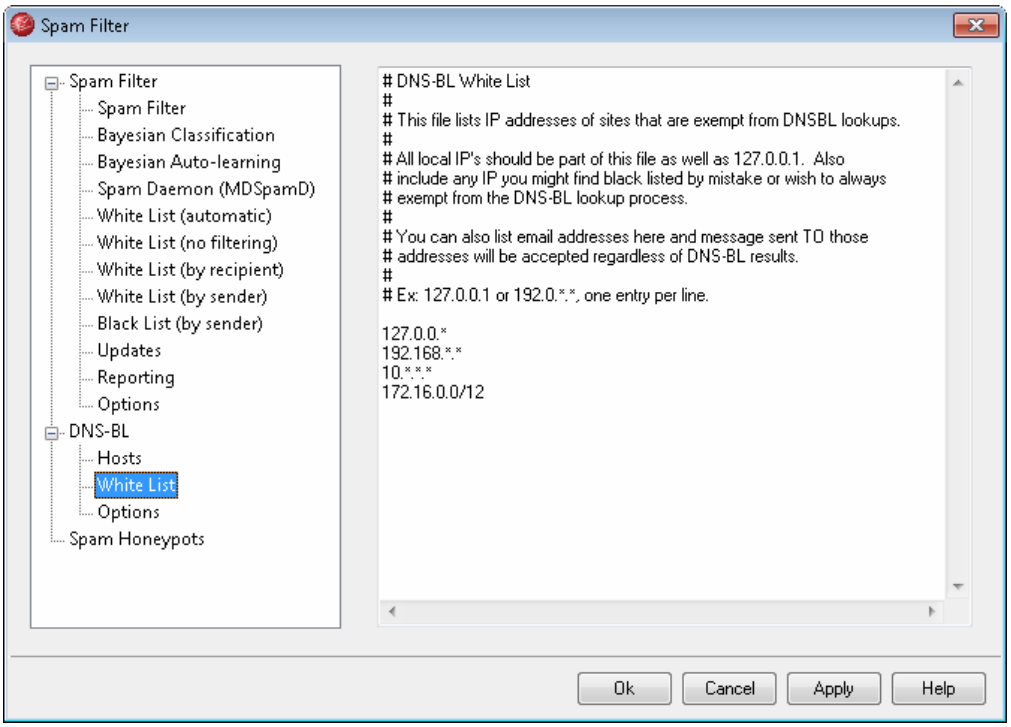
**DNS-BL host**
If you wish to add a new host to be queried for blacklisted IP addresses, enter it here.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Message**
This is the message that can be sent during the SMTP session when an IP address has been blacklisted by the corresponding DNS-BL host listed above. This message corresponds to the *...and respond with 'Message' rather than 'user unknown'* option located on the DNS-BL Options 267 screen.

**Add**
After entering a host and return message, click this button to add it to the DNS-BL hosts list.

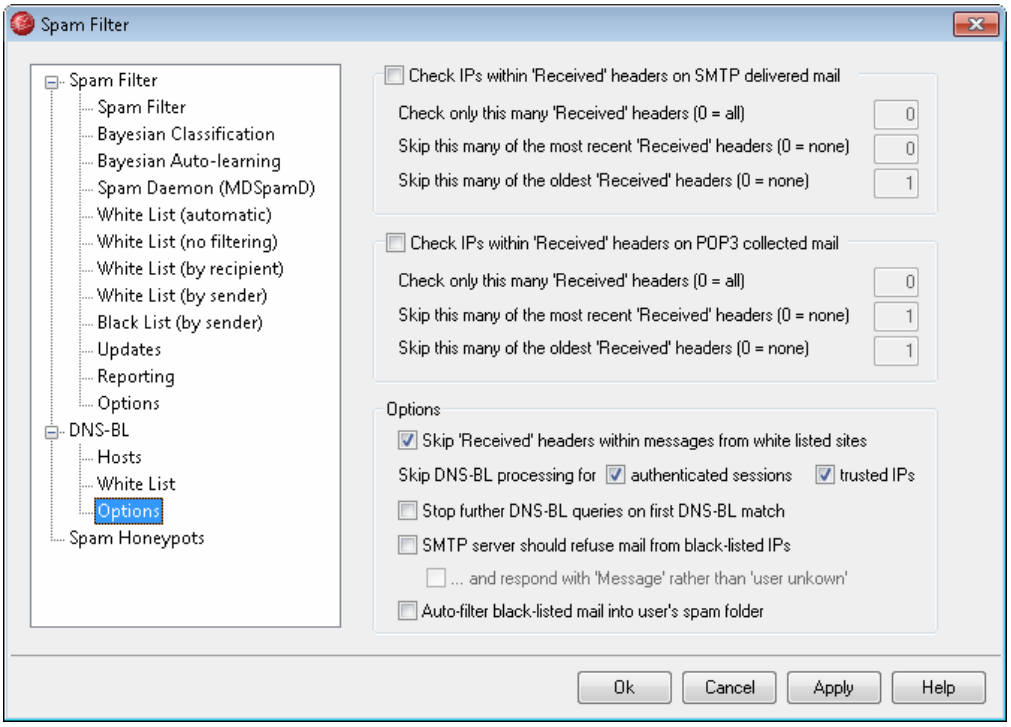
### 5.3.2.2 White List




Use this screen to designate IP addresses that will be exempt from DNS Black List queries. You should always include your local IP address range to prevent DNS-BL from looking up messages originating from local users and domains (i.e. `127.0.0.*`, `192.168.*.*`, and so on). Place one address on each line. Wildcards are permitted.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.2.3 Options




**Check IPs within 'Received' headers on SMTP delivered mail**
Click this switch if you want DNS Black Lists to check the IP address stamped in the "Received" headers of messages received via SMTP.

**Check only this many 'Received' headers (0 = all)**
Specify the number of "Received" headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all "Received" headers will be checked.

**Skip this many of the most recent 'Received' headers (0 =none)**
Use this option if you want DNS-BL to skip over one or more of the most recent Received headers when checking SMTP messages.

**Skip this many of the oldest 'Received' headers (0 =none)**
Use this option if you want DNS-BL to skip over one or more of oldest Received headers when checking SMTP messages.

**Check IPs within 'Received' headers on POP3 collected mail**
When this switch is enabled DNS-BL will check the IP address stamped in the " Received" headers of messages collected via DomainPOP and MultiPOP.

**Check only this many 'Received' headers (0 = all)**
Specify the number of 'Received' headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all 'Received' headers will be checked.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Skip this many of the most recent 'Received' headers (0 =none)**
Use this option if you want DNS-BL to skip over one or more of the most recent `Received` headers when checking DomainPOP and MultiPOP messages. Since it is often necessary to skip the most recent `Received` header on POP3 collected mail such as DomainPOP, this option has a default setting of "1".

**Skip this many of the oldest 'Received' headers (0 =none)**
Use this option if you want DNS-BL to skip over one or more of the oldest Received headers when checking DomainPOP and MultiPOP messages.

## Options

**Skip 'Received' headers within messages from white listed sites**
When this option is enabled, DNS-BL will not check the "Received" headers within messages coming from IP addresses that you have listed on the DNS-BL White List 266.

**Skip DNS-BL processing for:**

**authenticated sessions**
Click this checkbox if you want those sessions that were authenticated using the AUTH command to be exempt from DNS-BL queries.

**trusted IPs**
Click this checkbox if you want addresses that are listed on the Trusted Hosts 279 screen to be exempt from DNS-BL queries.

**Stop further DNS-BL queries on first DNS-BL match**
Oftentimes there are multiple hosts contained in the headers of each message that DNS-BL processes, and multiple DNS-BL services that are queried. By default, DNS-BL will continue to query these services for all hosts in the message regardless of the number of matches found. Click this option if you want DNS-BL to stop querying the services for any given message as soon as a match is found.

**SMTP server should refuse mail from black-listed IPs**
By default this box is unchecked, meaning that messages from blacklisted IP addresses will not be refused during the SMTP session, but will have an X-MDDNSBL-Result header inserted. You can then use the Content Filter to search for messages with this header and do with them as you please. You can also use the "*Auto-filter black-listed mail into user's spam folder*" option below to filter messages automatically into each user's spam folder. Check this box if you wish MDaemon to refuse messages from blacklisted IP addresses rather than flag them.

Because some IP addresses can be blacklisted by mistake, you should exercise caution before choosing to refuse messages rather than simply flagging them. It is also worth noting that in addition to flagging a message, you can adjust its spam score based on the DNS-BL results via the *DNS-BL match adds this many points to the spam score* option located on the Spam Filter 242.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...and respond with 'Message' rather than 'user unknown'**
Click this option if you want the specific Message you have assigned to the DNS-BL Host 265 to be passed during the SMTP session whenever an IP address is found to be blacklisted. Otherwise, a "user unknown" message will be passed instead. This option is only available if you have elected to use the "*SMTP server should refuse mail from black-listed IPs*" option above.

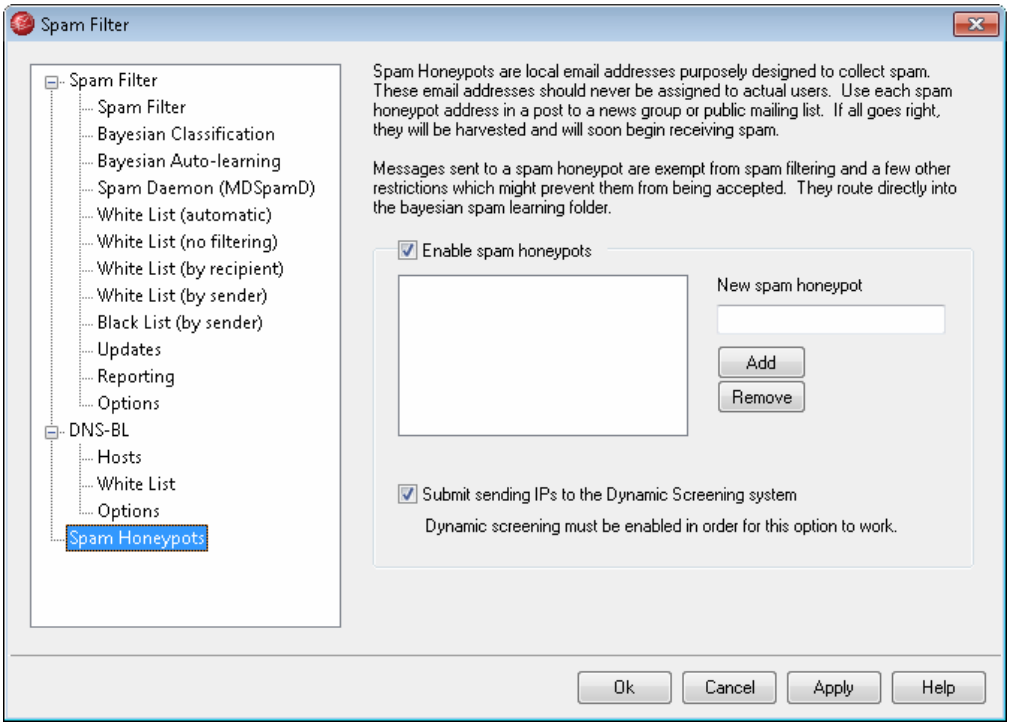
**Auto-filter black-listed mail into user's spam folder**
Click this option and a "Junk E-mail" IMAP folder will be created for all future user accounts that you add to MDaemon. MDaemon will also create a mail filter for each of those users, which will search for the X-MDDNSBL-Result header and then place messages containing that header into the user's spam folder. When you click this option you will also be asked whether or not you would like MDaemon to create this folder and filter for each of your already existing user accounts. See *Auto-generating a Spam Folder and Filter for Each Account* below.

## Auto-generating a Spam Folder and Filter for Each Account

MDaemon can automatically create a "Junk E-mail" IMAP mail folder for each account and generate a mail filter that will move messages into that folder whenever if finds the `X-MDDNSBL-Result` header. Whenever you click the *Auto-filter black-listed mail into user's spam folder* option, you will be presented with the option to create the folder and accompanying filter for all accounts. Simply choose "yes" on the dialog to create the folders and filters. Although not foolproof, this is an easy and generally reliable way to help your users quickly identify spam email messages—it can effectively prevent spam email from being mixed in with all of their legitimate email. They will only occasionally need to review the contents of their spam folder just to make sure that an important message doesn't accidentally get put there (which may sometimes occur). When creating the folders and filters for your accounts, if MDaemon finds that an account already has a filter that checks for the existence of the `X-MDDNSBL-Result` header then no action will be taken and no filter will be created for that account. If you want the name of the IMAP folder to be something other than "Junk E-mail", you can change the default setting by editing the *Default spam folder name* option located on the System 195 screen under `Setup » Preferences`.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.3.3 Spam Honeypots




Spam Honeypots (located at Security » Spam Filter » Spam Honeypots) is for designating local email addresses purposely designed to collect spam. These spam honeypots are not valid MDaemon accounts or address aliases and should never be used for sending or receiving legitimate email. But, by posting a honeypot address to a news group, public mailing list, or other source from which spammers often farm addresses, you should begin to see incoming messages addressed to the spam honeypots — you could also pull addresses from other spam that you have received addressed to other invalid local addresses. Because honeypots will never receive legitimate email, all incoming messages addressed to them will always be routed directly to your Bayesian spam trap folder for processing. Further, the IP addresses of the sending servers can optionally be added to the Dynamic Screening 306 system, banning future connections from those addresses for a designated period of time. All of this helps increase the probability of identifying and blocking spam in the future.

#### Spam Honeypots

This list contains all addresses that you have designated as Spam Honeypots.

**Enable spam honeypots**
This option is enabled by default. Uncheck this box if you wish to disable the spam honeypots feature.

**New spam honeypot**
To add a spam honeypot, enter the address here and click *Add*.

**Remove**
To remove a spam honeypot, select the desired address and then click Remove.

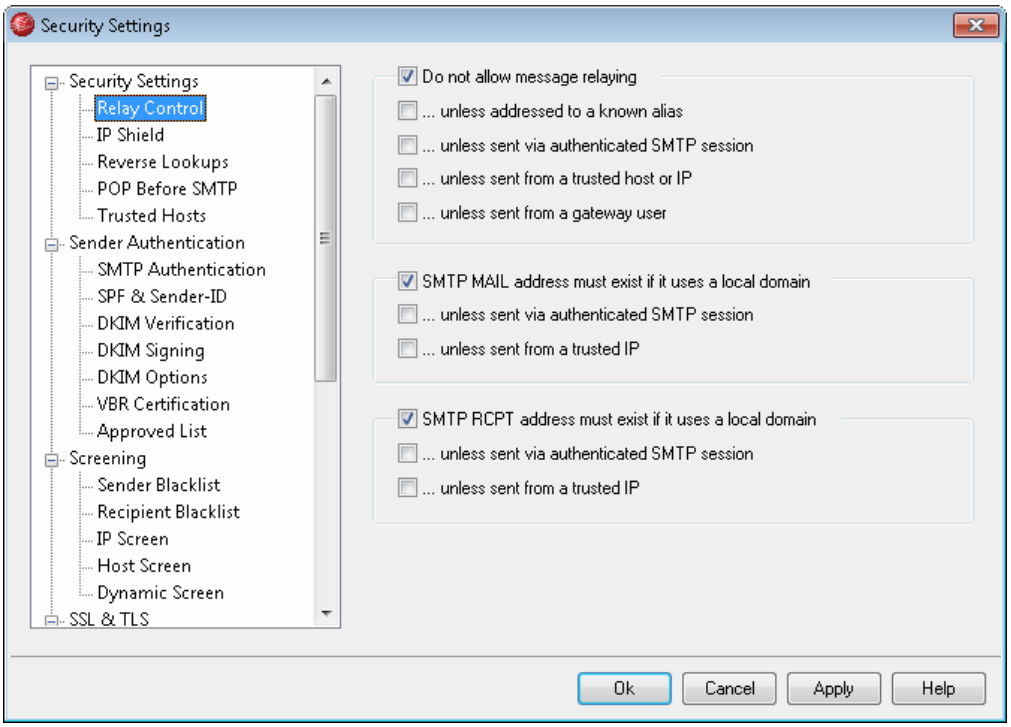
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Submit sending IPs to the Dynamic Screening system**
Check this box if you wish to submit to the Dynamic Screening 306 system all IP addresses from which a Spam Honeypots message arrives. The Dynamic Screen (located at Security » Security Settings » Screening » Dynamic Screen) must be enabled on your server before this feature will be available.

# 5.4 Security Settings

## 5.4.1 Security Settings

### 5.4.1.1 Relay Control




Use Relay Control at Security » Security Settings » Relay Control to define how your server reacts to mail relaying. When a message arrives at your mail server that is neither from nor to a local address, your server is being asked to relay (i.e. deliver) the message on behalf of another server. If you do not want your server to relay mail for unknown users, you can use the settings provided here to control that.

Relaying email indiscriminately for other servers could result in your domain being blacklisted by one or more DNS-BL services 264. Open relaying is greatly discouraged because spammers exploit open servers to hide their tracks.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Mail Relaying

**Do not allow message relaying**
When this option is enabled, MDaemon will refuse to accept messages for delivery that are both FROM and TO a non-local user.

**...unless addressed to a known alias**
Click this checkbox if you want MDaemon to relay mail for Aliases[398] regardless of your Relay settings.

**...unless sent via authenticated SMTP session**
When this checkbox is enabled, MDaemon will always relay mail when it is sent via an authenticated SMTP session.

**...unless sent from a trusted host or IP**
Enable this option is you wish to allow relaying when the mail is coming from a Trusted Host or Trusted IP address.

**...unless sent from a gateway user**
Enable this checkbox if you want MDaemon to permit mail relaying through domain gateways regardless of your Relay settings. This feature is disabled by default and isn't recommended.

### Account Verification

**SMTP MAIL address must exist if it uses a local domain**
Click this option is you wish to verify that the MAIL value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain or gateway.

**...unless sent via authenticated SMTP session**
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent via an authenticated SMTP mail session.

**...unless sent from a trusted host or IP**
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent from a Trusted IP address.

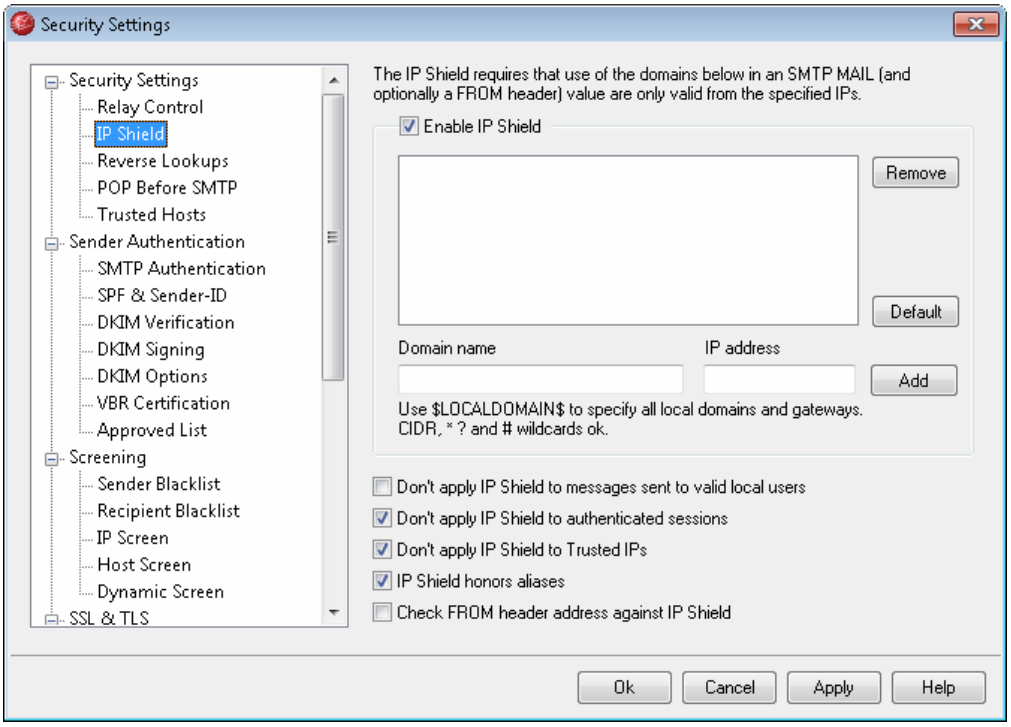
**SMTP RCPT address must exist if it uses a local domain**
Click this option is you wish to verify that the RCPT value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain.

**...unless sent via authenticated SMTP session**
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent via an authenticated SMTP mail session.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...unless sent from a trusted host or IP**
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent from a Trusted IP address.

### 5.4.1.2 IP Shield




The IP Shield, located under the Security » Security Settings menu, is a list of domain names and matching IP addresses that will be checked during the `MAIL From` command during the SMTP session. An SMTP session claiming to be from someone at one of the listed domains will be honored only if it is coming from one of the associated IP addresses. For example, suppose your domain name is example.com and your local LAN computers use IP addresses in the range from 192.168.0.0 to 192.168.0.255. With this information you can setup the IP Shield to associate the domain name example.com with the IP address range 192.168.0.* (wildcards are allowed). Thus anytime a computer connects to your SMTP server and states, "`MAIL FROM <someone@example.com>`", the SMTP session will continue only if the connecting computer has an IP address within the required range from 192.168.0.0 to 192.168.0.255.

**Enable IP Shield**

Clear this checkbox if you wish to disable the IP Shield. The IP Shield is enabled by default.

**Domain name**
Enter the domain name that you wish to associate with a specific IP address range. You can also use the `$LOCALDOMAIN$` macro to cover all local domains (including

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

gateways). If you use this macro it will not be necessary to keep the IP Shield up to date when local domains or gateways change. By default, entries are added to the IP Shield associating all reserved IP address ranges with `$LOCALDOMAIN$`.

**IP address**
Enter the IP address that you wish to associate with a domain name. You must enter this address in dotted decimal form.

**Add**
Click the *Add* button to add the domain and IP address range to the listing.

**Remove**
Click this button to remove the selected entries from the listing.

**Don't apply IP Shield to messages sent to valid local users**
Click this option if you want only those messages that are destined for a non-local user or invalid local user to be checked for a domain/IP match. This will prevent others from posing as one of your local users in order to relay their mail through your server, but it will save resources by not checking messages that are address to your users. If you enable both this option and the *IP Shield honors aliases* option below, messages to valid aliases will be accepted as well.

**Don't apply IP Shield to authenticated sessions**
When this control is active, the IP Shield restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be "Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message. This option is enabled by default.

**Don't apply IP Shield to Trusted IPs**
When this control is active, the IP Shield will not be applied when the connection is from a Trusted IP address 279. This option is enabled by default.

**IP Shield honors aliases**
Enable this option if you want the IP Shield to honor address aliases when checking domain/IP address shields. The IP Shield will translate an alias to the true account to which it points and thus honor it if it passes the shield. Without this option enabled, the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the Options screen 400 of Address Aliases — changing the setting here will be reflected there.

If you want incoming messages that are addressed to valid aliases to be exempt from IP Shielding then click both this option and the *Don't apply IP Shield to messages sent to valid local users* option above.

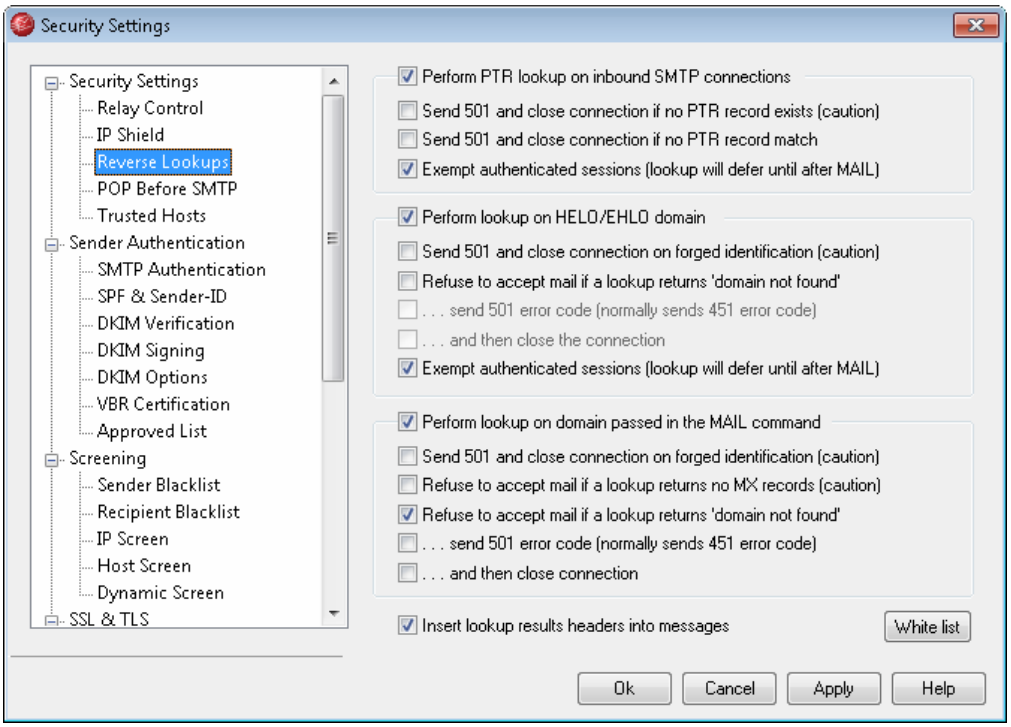
**Check FROM header address against IP Shield**
Check this box if you want the IP Shield to compare the address taken from the message's FROM header in addition to that taken from the SMTP MAIL value. This

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

option is disabled by default.

Using this option could cause problems with certain types of messages, such as those coming from mailing lists. It should therefore be enabled only if you are sure you need it.

### 5.4.1.3 Reverse Lookup




With the options on this screen, MDaemon can be configured to do a reverse lookup on the domain passed in the `HELO/EHLO` and `MAIL` commands. When performing the lookups MDaemon will attempt to acquire all of the MX and A record IP addresses for the given domain. Then the IP of the server making the connection is compared to this list in an attempt to determine whether the sender might be using a forged identity.

Oftentimes the sending mail server's IP address will not match any known MX or A records for a given domain and yet still be delivering the mail legitimately. The purpose of the Reverse Lookup process is therefore not to exclude mail but to include as much information as possible in the log files, and to provide the means whereby the postmasters can act according to their own local policies regarding these suspicious messages. To that end, an option exists that makes it possible for a special header to be inserted into all messages that do not pass a reverse lookup. The content filter system can then be used to determine the fate of messages containing the header.

You can also perform reverse lookups on pointer records (PTR) of incoming IP addresses. When using this option the connection can be aborted or a warning header inserted into the message if the incoming IP address does not match any PTR record.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Finally, it is generally agreed that accepting mail from sources that identify themselves by using a domain that does not exist should be optional. Therefore, a switch exists that makes it possible for you to refuse messages for which the reverse lookup process returns a "domain not found" message from the DNS server. In such cases, MDaemon will return a `451` error code, refuse to accept the message, and then allow the SMTP session to progress. However, should you wish to return a `501` error code, close the socket connection, or do both, other switches are provided for those purposes.

Trusted IP addresses and localhost (127.0.0.1) are always exempt from reverse lookups.

**Perform PTR lookup on inbound SMTP connections**
Enable this option if you want MDaemon to perform pointer record lookups on all inbound SMTP connections.

**...send 501 and close connection if no PTR record exists (caution)**
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if no PTR record exists for the domain.

**...send 501 and close connection if no PTR record match**
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if the result of a pointer record lookup fails to match.

**Exempt authenticated sessions (lookup will defer until after MAIL)**
Click this option if you wish to defer the PTR lookup on inbound SMTP connections until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

**Perform lookup on HELO/EHLO domain**
Click this box if you want a lookup to be performed on the domain name that is reported during the `HELO/EHLO` portion of the session. The `HELO/EHLO` command is used by the client (sending machine) to identify itself to the server. The domain name passed by the client in this command is used by the server to populate the `from` portion of the `Received` header.

**Perform lookup on value passed in the MAIL command**
Enabling this switch will cause a lookup to be performed on the domain name that is passed during the `MAIL` command portion of the mail transaction. The address passed in the `MAIL` command is supposed to be the reverse-path for the message, and is usually the mailbox from which the message is originating. Sometimes, however, it is the address to which error messages should be directed instead.

**...send 501 and close connection on forged identification (caution)**
Click this check box if you want a 501 error code to be sent and then the connection closed when the result of a lookup appears to be a forged identification.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

When the result of a reverse lookup states that the server is using a forged identification, this result may frequently be incorrect. It is very common for mail servers to identify themselves with values that do not match their IP addresses. This can be due to ISP limitations and restrictions and other legitimate reasons. For this reason, you should exercise caution before enabling this option. It is likely that using this option could result in your server refusing some legitimate messages.

**Refuse to accept mail if a lookup returns no MX records (caution)'**
Check this box if you wish to refuse MAIL from domains that do not have MX records. This option is disabled by default and should be used with caution, because domains do not need MX records in order to exist, be valid, or send/receive mail.

**Refuse to accept mail if a lookup returns 'domain not found'**
When a lookup results in "`domain not found`", enabling this option will cause the message to be refused with a `451` error code (Requested action aborted: local error in processing) and then the session will be allowed to progress normally to its conclusion.

**...send 501 error code (normally sends 451 error code)**
Enable this checkbox if you want the error code that is sent in response to a "domain not found" result to be `501` (syntax error in parameters or arguments) instead of `451`.

**...and then close the connection**
Click this checkbox if you want the connection to be closed immediately instead of allowed to progress when "`domain not found`" is the result of the reverse lookup.

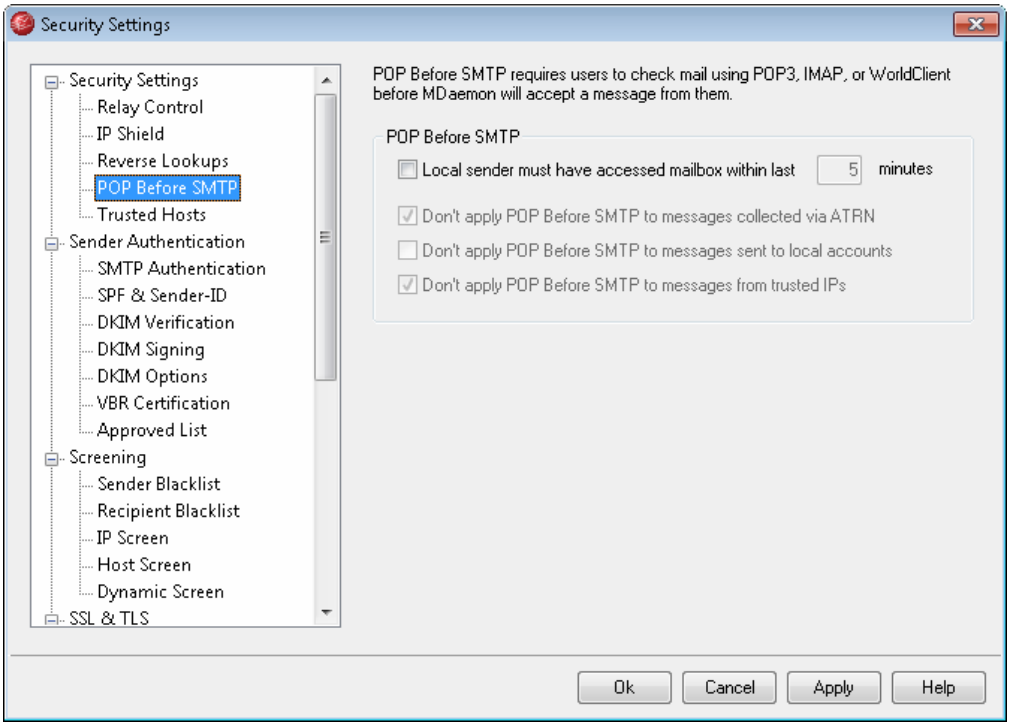
**Exempt authenticated sessions (lookup will defer until after MAIL)**
Click this option if you wish to defer the lookup until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

**Insert lookup results headers into messages**
Click this checkbox if you want special headers containing the results of the reverse lookups to be included in the message headers. MDaemon will insert one or more of the following headers, depending on which types of lookups you have set MDaemon to perform: "`X-MDPtrLookup-Result:`", "`X-MDHeloLookup-Result:`", and "`X-MDMailLookup-Result:`".

**White list**
Click this button to open the Reverse Lookup White List dialog. On it you can designate IP addresses, domains, and hosts that you wish to be exempt from reverse lookups.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.1.4 POP Before SMTP




#### POP Before SMTP

**Local sender must have accessed mailbox within last [XX] minutes**
With this feature enabled, whenever a message is purported to be from a local user, that user account must have logged in and checked its local mailbox within the specified number of minutes before it will be allowed to send mail.

**Don't apply POP Before SMTP to messages collected via ATRN**
Check this box if you want messages collected via ATRN 466 to be exempt from the POP Before SMTP restriction.

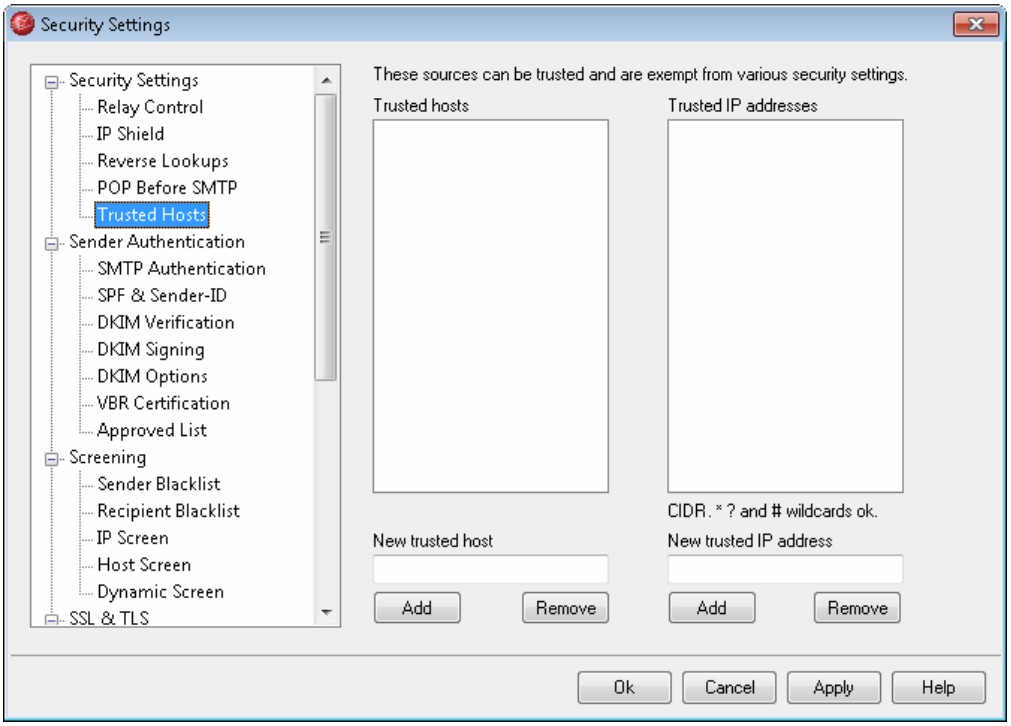
**Don't apply POP Before SMTP to messages sent to local accounts**
Click this checkbox if you want messages that are sent from one local user to another to be exempt from the POP Before SMTP requirement. Ordinarily, MDaemon will enforce the requirement as soon as the sender is known, but when this control is enabled MDaemon will wait until the recipient of the message is revealed before determining whether or not it is required.

**Don't apply POP Before SMTP to messages from trusted IPs**
If this checkbox is enabled, messages arriving from an IP address listed on the Trusted Hosts 279 screen will be exempt from POP Before SMTP.

You can exempt authenticated sessions from the POP Before SMTP restriction via an option on the SMTP Authentication 280 screen.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.1.5 Trusted Hosts




On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted Hosts," "Trusted Domains," or "Trusted IPs" will be exceptions to or exempt from those options. The hosts and IP addresses you list on this screen are the ones to which those options refer.

**Trusted hosts**
This is the list of hosts that will be exempt from certain designated security options.

**New trusted host**
Enter a new domain name to be added to the *Trusted hosts* list.

**Add**
Click this button to add the new domain to the *Trusted hosts* list.

**Remove**
Click this button to remove the selected entries from the *Trusted hosts* list.

**Trusted IP addresses**
This is the list of IP addresses that will be exempt from certain designated security options.

**New trusted IP address**
Enter a new IP address to be added to the *Trusted IP Addresses* list.

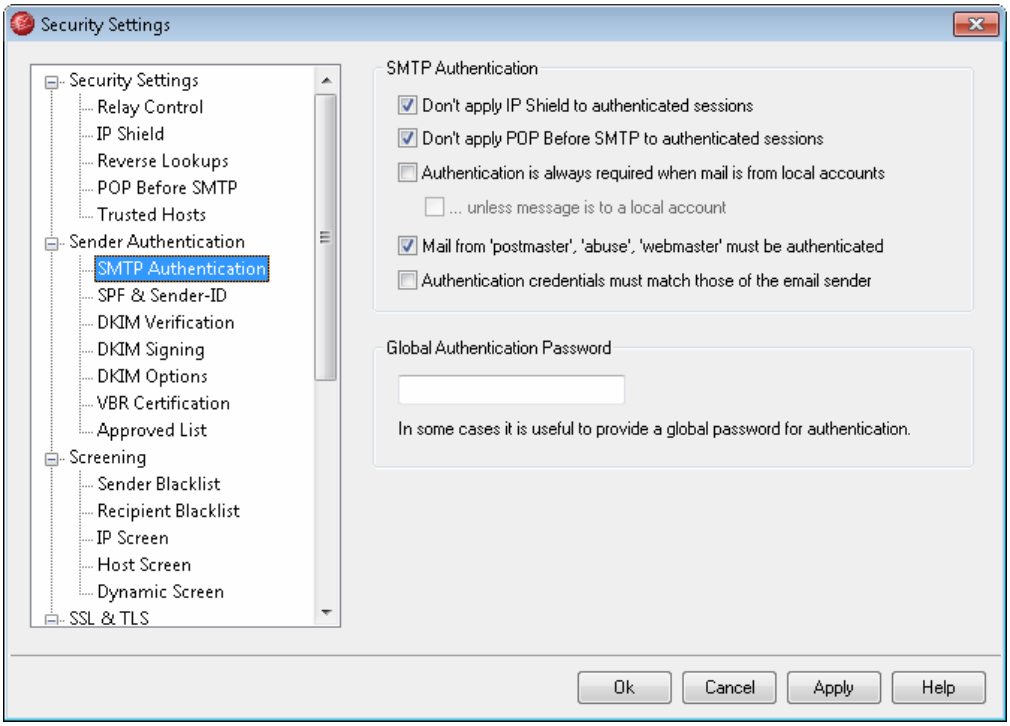
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Add**
Click this button to add the new IP address to the *Trusted IP Addresses* list.

**Remove**
Click this button to remove the selected entries from the *Trusted IP Addresses* list.

## 5.4.2 Sender Authentication

### 5.4.2.1 SMTP Authentication




**SMTP Authentication**

**Don't apply IP Shield to authenticated sessions**
When this control is active, the IP Shield 273 restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be "Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message. This option is enabled by default.

**Don't apply POP Before SMTP to authenticated sessions**
If you are utilizing the POP Before SMTP 278 security feature, you can click this option to make authenticated users exempt from this restriction. An authenticated user will not need to check his or her email before sending messages.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Authentication is always required when mail is from local accounts**
When this option is enabled and an incoming message claims to be from one of MDaemon's domains, the account must first be authenticated or MDaemon will refuse to accept the message for delivery.

**...unless message is to a local account**
If you are requiring authentication when a message is from a local sender, but wish to skip the authentication restriction when the recipient is local as well, then click this option. Note: this may be necessary in some situations where you require some of your users to use different mail servers for outgoing and incoming mail.

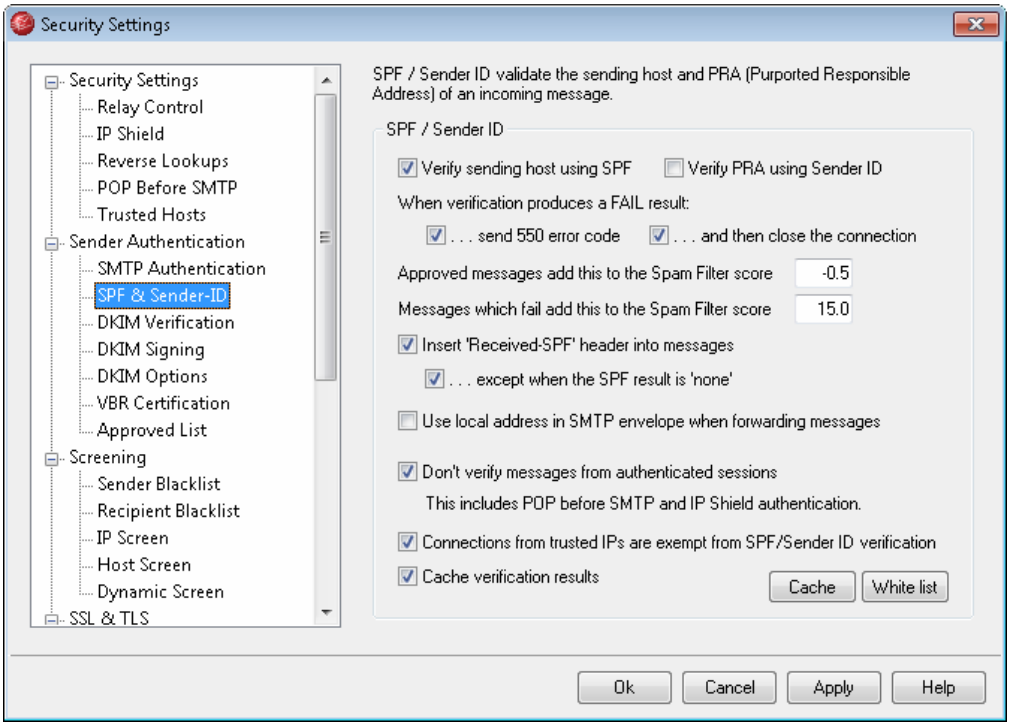
**Mail from 'Postmaster', 'abuse', 'webmaster' must be authenticated**
Click this checkbox to require messages claiming to be from one of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send mail through your system. This option will prevent them and other unauthorized users from being able to do so. This option is mirrored on the Options screen 400 of Address Aliases. Changing the setting here will change it there as well.

**Authentication credentials must match those of the email sender**
Use this option if you wish to require a sender to use only his own credentials for authentication. So, for example, *user1@example.com* would only be allowed to authenticate using the *user1@example.com* account credentials. If he attempted to authenticate using *user2@example.com* then it would not be allowed, even if the *user2@example.com* credentials were valid. This option is disabled by default.

**Global Authentication Password**
Some configurations may require a global authentication password. If you require that then designate that password here.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.2.2 SPF & Sender ID




MDaemon supports both Sender Policy Framework (SPF) and Sender ID Framework (SIDF) to help verify sending servers and protect against spoofing and phishing, which are two common types of email forgery in which the sender of the message attempts to make the message appear to be coming from someone else.

Many domains publish MX records in the Domain Name System (DNS) to identify the locations permitted to receive mail for them, but this doesn't identify the locations allowed to *send* mail for them. SPF is a means whereby domains can also publish sender records to identify those locations authorized to send messages. By performing an SPF lookup on incoming messages, MDaemon can attempt to determine whether or not the sending server is permitted to deliver mail for the purported sending domain, and consequently determine whether or not the sender's address may have been forged or "spoofed". Sender ID is related to SPF, but it is more complex in order to more reliably determine the actual domain purported to have sent the message, and to reduce the likelihood of incorrect results.

Use the options on this tab to configure your server's SPF and Sender ID settings.

For more information on SPF, visit:

http://spf.pobox.com

For more information on Sender ID, visit:

http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## SPF / Sender ID

**Verify sending host using SPF**
When this option is enabled, MDaemon will perform queries for SPF data on the sending host of any incoming messages that do not come from white listed IP addresses or exempt sessions, such as authenticated connections or trusted IP addresses (when those exemptions have been enabled). The host MDaemon will verify is taken from the `MAIL` value passed during SMTP processing This SPF verification option is enabled by default.

**Verify PRA using Sender ID**
Enable this option if you wish to use the Sender ID framework to verify incoming messages. MDaemon will identify the Purported Responsible Address (PRA) of the incoming message through careful inspection of its headers and then verify whether or not the message originated from that location. The PRA is the most recent address purported to be responsible for the message, which may or may not be its original sender.

**When verification produces a FAIL result:**

**...send 550 error code**
Click this check box if you want a 550 error code to be sent when the result of the SPF/Sender ID query is "Fail".

**...and then close the connection**
Enable this option if you want the connection to be closed immediately after sending the 550 error code.

**Approved messages add this to the Spam Filter score**
Specify the amount that you wish to add to a message's Spam Score when SPF/Sender ID confirms that it originated from a domain found on the Approved List 298.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for the approved messages.

**Messages which fail SPF add this to the Spam Filter score**
Specify the amount that you wish to add to the message's Spam Score when it fails to pass SPF/Sender ID verification.

**Insert 'Received-SPF' header into messages**
Click this option if you want a "Received-SPF" header to be inserted into each message.

**...except when the SPF result is 'none'**
Enable this option if you do not wish the "Received-SPF" header to be inserted into a message when the result of the SPF query is "none".

**Use local address in SMTP envelope when forwarding messages**
Click this option if you want all mail forwarded by MDaemon to use a local address in

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the SMTP envelope. This helps reduce problems associated with forwarding. Normally, forwarded messages are sent using the email address of the original sender and not the email address that is actually doing the forwarding. In some situations, using a local address may be necessary in order to prevent the receiving server from falsely identifying the forwarded message as having a "spoofed" address.

### Verification Options

**Don't verify messages from authenticated sessions**
Click this check box if you wish authenticated connections to be exempt from SPF/ Sender ID queries. Authenticated sessions include those verified via SMTP Authentication 280, POP before SMTP 278, or the IP Shield 273.

**Connections from trusted IPs are exempt from SPF/Sender ID verification**
Enable this option if you want connections from trusted IP addresses 279 to be exempt from SPF/Sender ID verification.

**Cache verification results**
Click this option if you wish to temporarily cache the results of SPF queries.

**Cache**
This button opens the SPF cache.

**White List**
Click this button to open the SPF white list on which you can designate IP addresses that you wish to exempt from SPF lookups.

## 5.4.2.3 DomainKeys Identified Mail

DomainKeys (DK) and DomainKeys Identified Mail (DKIM) are cryptographic email verification systems that can be utilized to prevent spoofing (forging another person's email address in order to pose as a different message sender). Additionally, because most junk email (spam) messages contain spoofed addresses, DK/DKIM can help greatly in the reduction of spam even though the specifications weren't specifically designed to be an anti-spam tool. DK/DKIM can also be used to ensure the integrity of incoming messages, or ensure that the message hasn't been tampered with between the time it left the signing mail server and arrived at yours. In other words, with DK/DKIM cryptographic verification the receiving server can be certain that the arriving message is from the server that signed it, and that no one changed that message in any way.

In order to ensure the validity and integrity of messages, DK/DKIM uses a public and private key-pairs system. An encrypted public key is published to the sending server's DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the receiving server sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's cryptographic signature to determine its validity. If the incoming message cannot be verified then the receiving server knows it contains a spoofed address or has been tampered with or changed. A failed message can then be rejected, or it can be accepted but have its spam score adjusted.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

To configure MDaemon to verify incoming cryptographically signed messages, use the options provided on the DKIM Verification 285 screen. To configure MDaemon to sign outgoing messages, use the options provided on the DKIM Signing 289 screen. Both are located under the Sender Authentication section of the Security Settings dialog, at: Security » Security Settings » Sender Authentication. MDaemon's main interface 30 includes a "DK/DKIM" tab (located under the Security tab) that can be used for monitoring DK/DKIM activity in real time, and you can log DK/DKIM activity using the option at: Setup » Default Domain/Servers » Logging » Options.

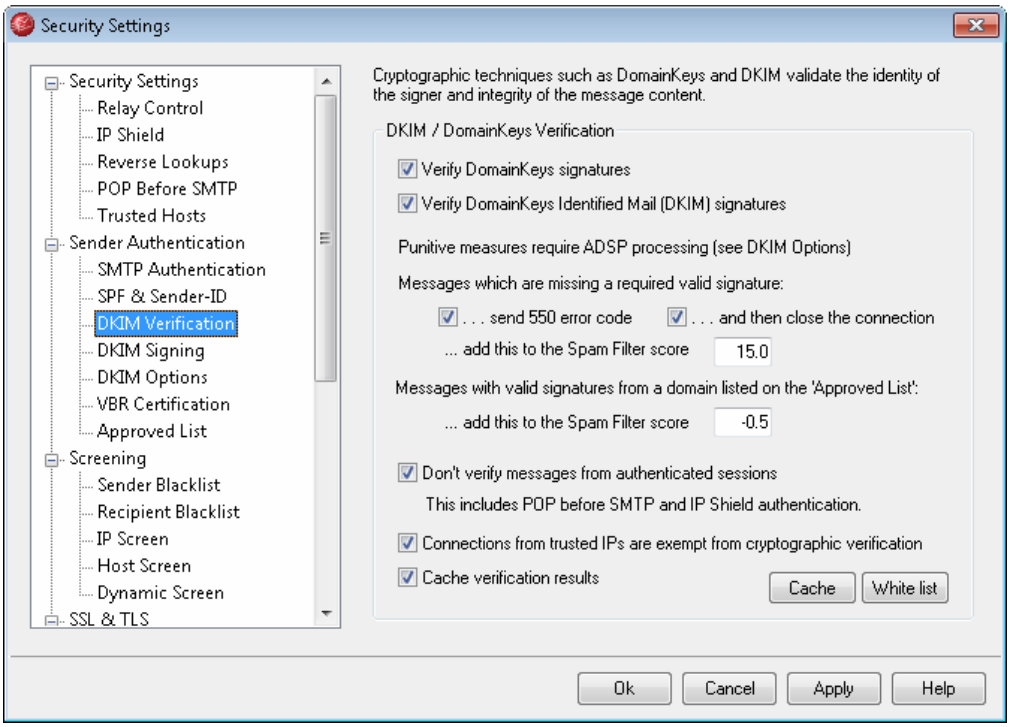
**See:**

**DKIM Verification** 285
**DKIM Signing** 289
**DKIM Options** 292

For more on DomainKeys Identified Mail, visit: http://www.dkim.org/.

For more on DomainKeys, visit: http://antispam.yahoo.com/domainkeys.

### 5.4.2.3.1 DKIM Verification




Use this screen to configure MDaemon to verify DomainKeys Identified Mail (DKIM) and/or DomainKeys (DK) signatures in incoming remote messages. When this feature is enabled and an incoming message has been cryptographically signed, MDaemon will retrieve the public key from the DNS record of the domain taken from the signature and

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

then use that key to test the message's DKIM or DK signature to determine its validity.

If the signature passes the verification test, the message will continue on to the next step in the regular delivery process. Additionally, if the domain taken from the signature also appears on the Approved List 298, the message's Spam Filter score will receive a beneficial adjustment.

If a message has no signature, or if the signature is invalid, MDaemon will retrieve the Author Domain Signing Practices (ADSP) record of the domain in the `From` header to determine whether or not all of that domain's messages should be signed. If the ADSP record indicates that a valid signature is required and the public key indicates that the signer is not merely testing DKIM, the message will receive a "Fail" result and be treated accordingly—it can be rejected outright or accepted but have its Spam Filter score adjusted upward.

Finally, if a site's ADSP record uses a syntax unknown to MDaemon, if no record exists at all, or if the ADSP option located on the DKIM Options 292 screen is disabled, then no punitive measures will be taken. The unsigned or invalidly signed message will be treated as if the domain signs only some of its messages.

For more on DKIM see: http://www.dkim.org/

### DKIM / DomainKeys Verification

**Verify DomainKeys signatures**
Click this option to enable DomainKeys verification of incoming remote messages.

**Verify DomainKeys Identified Mail (DKIM) signatures**
Click this option to enable DomainKeys Identified Mail verification of incoming remote messages. If you have configured MDaemon to verify both DKIM and DK signatures, and a given message contains both types of signatures, then no DK verification will be attempted if a DKIM signature produces a "pass" result. This option is required if you have SecurityPlus for MDaemon installed and wish to use its Urgent Updates 151 feature.

### Verification Outcomes

**Messages which are missing a required valid signature:**
The following punitive measures can only be applied to messages when the Author Domain Signing Practices (ADSP) option is enabled on the DKIM Options 292 screen. When the ADSP option is disabled, no messages will be rejected or scored negatively by DKIM verification, regardless of these settings.

**...send 550 error code**
When the ADSP record indicates that a valid signature is required, any message without one will be rejected—MDaemon will return the `550` code and reject the message during the SMTP process. If, however, the signer's public key indicates that the signer is merely testing DK/DKIM, the message will be processed normally.

**...and then close the connection**
Click this option if you wish to close the connection to the sending server

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

when a message is rejected according to the previous option. If this option is disabled then the message will still be rejected according to the previous option but the connection will be allowed to continue.

**...add this to the Spam Filter score**
When the ADSP record indicates that a valid signature is required, any message without one will have this value added to its Spam Filter score. If, however, you have enabled the "*...send 550 error code*" option above, the message will be rejected as invalid without having to be processed through the Spam Filter. In all cases, if the signer's public key indicates that the domain is "testing," no action will be taken—the Spam Filter score will not be modified.

Using this option could still cause a message to be rejected if the resulting Spam Filter score exceeds the SMTP rejection threshold designated on the Spam Filter 242 screen.

**Messages with valid signatures from a domain listed on the 'Approved List':**

**...add this to the Spam Filter score**
The value specified here will be added to the Spam Filter score of any DK or DKIM signed messages that receive a "Pass" result when the domain taken from the signature appears on the Approved List 298. When a message's signature is verified but the domain is not on the Approved List, the Spam Filter score will not be adjusted—the verified signature will have no effect on the score. However, normal Spam Filter processing and scoring will still be applied to that message.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for messages containing a valid cryptographic signature when the domain taken from the signature is on the Approved List 298. MDaemon's default value for this option is `-0.5`.

## Verification Options

**Don't verify messages from authenticated sessions**
Click this option if you want to exempt messages from cryptographic verification when the message session is authenticated. Authenticated sessions include those verified via SMTP Authentication 280, POP before SMTP 278, or the IP Shield 273.

**Connections from trusted IPs are exempt from cryptographic verification**
Use this option if you want connections from trusted IP addresses 279 to be exempt from cryptographic verification.

**Cache verification results**
Click this option if you wish to cache the DK/DKIM information found during the DNS lookup. By temporarily caching the information contained in a domain's DNS record, you can increase the efficiency of processing DK/DKIM signed messages that arrive in the near future from the same domain.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Cache**
This button opens the DomainKeys cache. When using the *Cache verification results* option above, this file will list any currently cached information.

**White list**
Click this button to open the exception list. Messages originating from any IP addresses specified on the list will not be subject to cryptographic verification.

## Authentication-Results header

Whenever a message is authenticated using SMTP AUTH, SPF, DomainKeys, or DomainKeys Identified Mail, MDaemon will insert the Authentication-Results header into the message listing the results of the authentication process. If MDaemon is configured to accept messages even when they fail authentication, then the Authentication-Results header will contain a code to identify the reason for the failure.

There is ongoing work via the Internet Engineering Task Force (IETF) on this header and the authentication protocols mentioned in this section. You can find more information on this at the IETF web site, located at: http://www.ietf.org/.

## DK/DKIM Headers in Mailing List Messages

By default, MDaemon strips DK/DKIM signatures from incoming list messages because those signatures can be broken by changes made to the message headers or content during list processing. If you would like MDaemon to leave signatures in list messages, you can configure it to do so by manually setting the following option in the `MDaemon.ini` file:

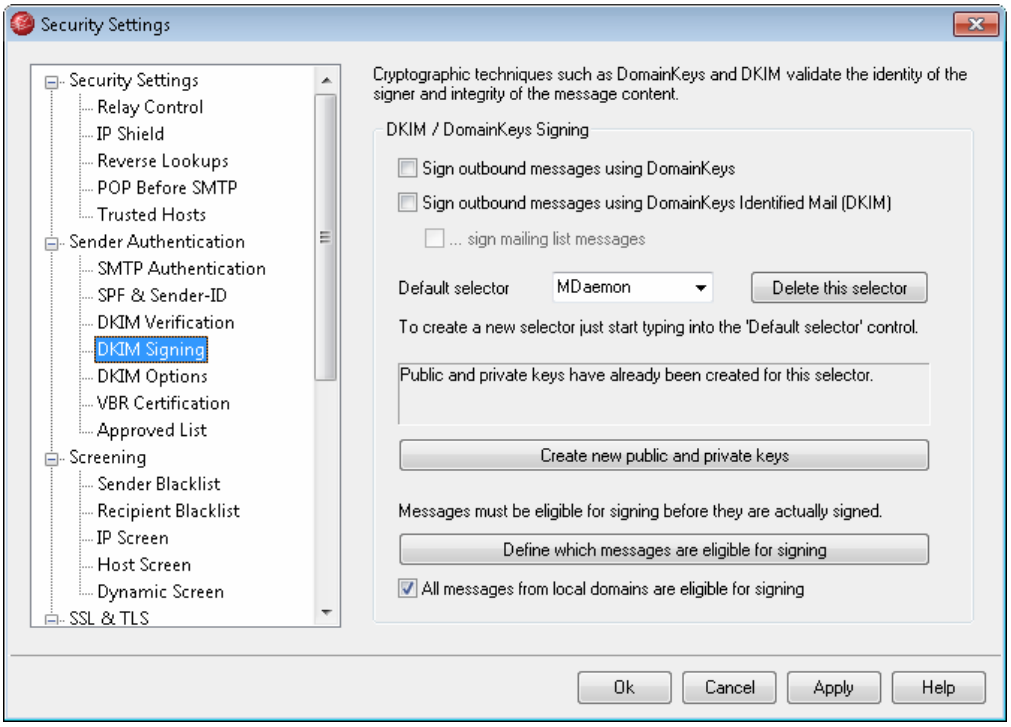
```
[DomainKeys]
StripSigsFromListMail=No (default is "Yes")
```

**See:**

**DomainKeys Identified Mail** 284
**DKIM Signing** 289
**DKIM Options** 292

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.2.3.2 DKIM Signing




Use the options contained on the DKIM Signing screen to control whether or not some outgoing messages will be cryptographically signed, the method that will be used to sign them (DK and/or DKIM), and to designate which messages should be signed. You can also use this screen to designate selectors and generate corresponding public and private keys suitable for use with the DK and DKIM specifications. A default selector ("MDaemon") and a default public and private key are created for you automatically on startup. All keys are unique—they are never the same from one site to another, regardless of the selector specified. By default, keys are generated with a secure bit depth of 1024 bits.

#### DKIM / DomainKeys Signing

**Sign outgoing messages using DomainKeys**
Click this option if you wish MDaemon to use DomainKeys to cryptographically sign some outgoing messages. In order for a message to be signed, it must meet the criteria designated under the *Define which messages are eligible for signing* button and be received by MDaemon for delivery on an authenticated session. There is also a Content Filter action, "*Sign with DomainKeys selector...*" that you can use to cause messages to be signed.

**Sign outgoing messages using DomainKeys Identified Mail (DKIM)**
Click this option if you wish to use DomainKeys Identified Mail to cryptographically sign some outgoing messages. In order for a message to be signed, it must meet the criteria designated under the *Define which messages are eligible for signing* button and be received by MDaemon for delivery on an authenticated session. There is also a Content Filter action, "*Sign with DKIM selector...*" that you can use to cause messages to be signed.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**...sign mailing list messages**
Click this check box if you wish to cryptographically sign all outgoing Mailing List messages. Because MDaemon will sign all mail to all of your lists, you do not need to use the "*Define which messages are eligible for signing*" option to authorize them for cryptographic signing.

Signing list mail requires content filter processing for each list message after "cracking" the list. This could affect server performance when dealing with large and highly active mailing lists.

**Default selector**
From the drop-down list, choose the selector whose corresponding public/private key pair you wish to use when signing messages. If you wish to create a new key pair with a different selector, type the desired selector name here and click "*Create new public and private keys*" below. If you wish to sign some messages using an alternate selector, designate a specific selector under the "*Define which messages are eligible for signing*" option, or create a Content Filter rule using the "*Sign with DKIM selector...*" or "*Sign with DomainKeys selector...*" action.

**Delete this selector**
Click this button if you wish to delete a selector. Follow the on-screen instructions that appear.

**Create new public and private keys**
Click this button to generate a public/private key pair for the selector specified above. A public/private key pair will be generated for the selector, and the file `dns_readme.txt` will be generated and automatically opened. This file contains example DK/DKIM data that you will need to publish to your domain's DNS records listing your DK/DKIM Policy and the public key for the designated selector. The file lists samples for both testing and not testing status, and for whether you are signing all messages or just some messages originating from your domain. If you are currently testing DK/DKIM or this selector, then you will need to use the information contained in the Testing entries for either the Policy or the selector, depending on what you are testing. Otherwise you will need to use the Not Testing entries.

All keys are stored in `PEM` format, and all selectors and keys are stored under the `\MDaemon\Pem` folder in the following way:

```
\MDaemon\Pem\<Selector>\rsa.public - public key for this selector
\MDaemon\Pem\<Selector>\rsa.private - private key for this selector
```

The files contained in these folders are not encrypted or hidden, but they contain RSA private encryption keys that should never be accessed by anyone without permission. You should therefore take steps to secure these folders and subfolders using your OS tools.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Define which messages are eligible for signing**
When you have enabled one or both of the *Sign outgoing messages...* options above, click this button to edit the `DKSign.dat` file, which contains the list of domains and addresses that MDaemon will use to determine whether or not a message should be signed. For each address listed you must designate whether or not the message should be `To` or `From` that address in order for it to qualify to be signed, or you can designate some other header such as "`Reply-To`" or "`Sender`". Optionally, you can designate a selector for each entry, which will be used when signing a message that matches that entry. Finally, you can specify an optional signing domain to be used in the "d=" tag within the signature header. This can be useful, for example, when you have multiple sub-domains signing messages. In such cases you could use the "d=" tag to tell the receiving servers to look for the DK/DKIM keys in a single domain's DNS record thus making it possible for you to manage all of the keys in one record rather than having to manage separate records for each sub-domain. Wildcards are permitted in domains and addresses.

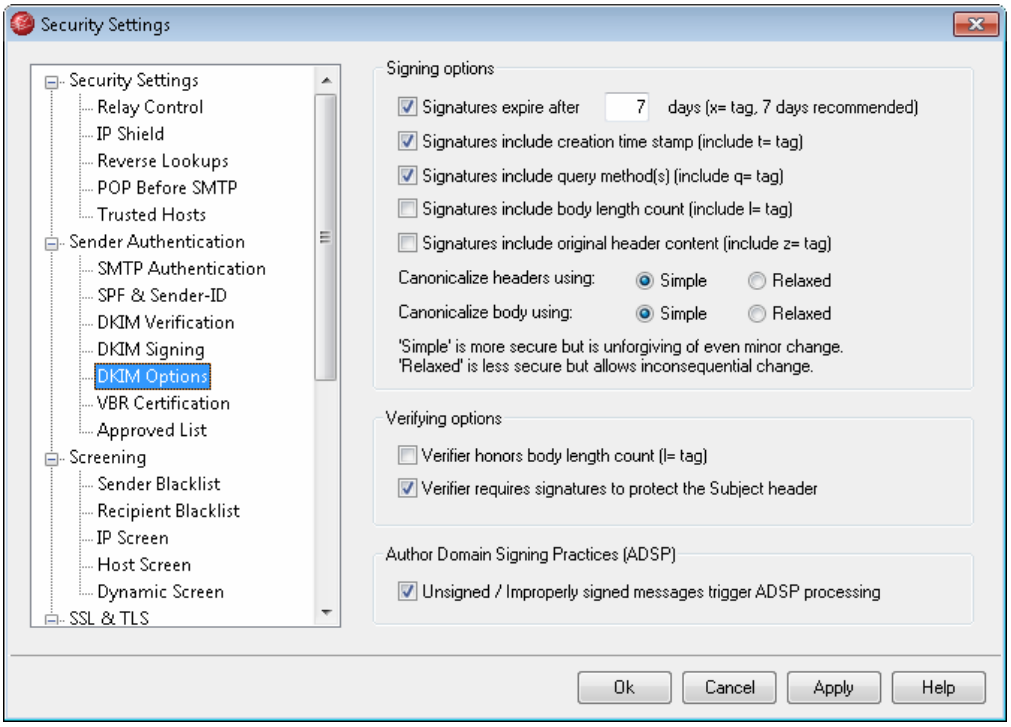
**All messages from local domains are eligible for signing**
Use this option if you wish to make all messages from your local domains eligible for signing. If you use this option then you do not need to add any of your local domains to the eligibility list (i.e. the `DKSign.dat` file) unless you wish to designate a specific selector or "`d=`" tag to be used when signing a specific domain's messages. This option is enabled by default.

**See:**

**DomainKeys Identified Mail** 284
**DKIM Options** 292
**DKIM Verification** 285

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.2.3.3 DKIM Options




#### Signing Options

**Signatures expire after [XX] days ("x=" tag, 7 days recommended)**
If you wish to limit the number of days that a DKIM signature can be considered valid, activate this option and specify the desired number of days. Messages with expired signatures will always fail verification. This option corresponds to the signature's "x=" tag. This option is enabled by default, with the value set to 7 days.

**Signatures include creation time stamp (include "t=" tag)**
When this option is enabled, the signature creation time stamp ("t=" tag) will be included in the signature. This is enabled by default.

**Signatures include query method(s) (include "q=" tag)**
By default this option is enabled. It causes the signature to include the query method tag (e.g. "q=dns").

**Signatures include body length count (include "l=" tag)**
Enable this option if you wish to include the body length count tag in DKIM signatures.

**Signatures include original header content (include "z=" tag)**
Click this option if you wish to include the "z=" tag in the DKIM signature. This tag will contain a copy of the message's original headers. This can potentially make signatures quite large.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Canonicalization

Canonicalization is a process whereby the message's headers and body are converted into a canonical standard and "normalized" before the DKIM signature is created. This is necessary because some email servers and relay systems will make various inconsequential changes to the message during normal processing, which could otherwise break the signature if a canonical standard was not used to prepare each message for signing. Currently there are two canonicalization methods used for DKIM signing and verification: Simple and Relaxed. Simple is the strictest method, allowing little to no changes to the message. Relaxed is more forgiving than Simple, allowing several inconsequential changes.

**Canonicalize headers using: Simple, Relaxed**
This is the canonicalization method used for the message headers when signing the message. Simple allows no changes to the header fields in any way. Relaxed allows for converting header names (not header values) to lower case, converting one or more sequential spaces to a single space, and other innocuous changes. The default setting is "Simple."

**Canonicalize body using: Simple, Relaxed**
This is the canonicalization method used for the message body when signing the message. Simple ignores empty lines at the end of the message body—no other changes to the body are allowed. Relaxed allows for blank lines at the end of the message, ignores spaces at the end of lines, reduces all sequences of spaces in a single line to a single space character, and other minor changes. The default setting is "Simple."

### Verifying Options

**Verifier honors body length count ("l=" tag)**
When this option is enabled, MDaemon will honor the body length count tag when it is found in an incoming message's DKIM signature. When the actual body length count is greater than the value contained in this tag, MDaemon will only verify the amount specified in the tag — the remainder of the message will remain unverified. This indicates that something was appended to the message, and consequently that unverified portion could be considered suspect. When the actual body length count is less than the value contained in this tag, the signature will not pass verification (i.e. it will receive a "FAIL" result). This indicates that some portion of the message was deleted, causing the body length count to be less than the amount specified in the tag.

**Verifier requires signatures to protect the Subject header**
Enable this option if you wish to require the DKIM signature of incoming messages to protect the Subject header.

### Author Domain Signing Practices (ADSP)

**Unsigned/Improperly signed messages trigger ADSP processing**
Enable this option if you wish to query for and honor Author Domain Signing Practices (ADSP) records when an incoming message is unsigned or improperly signed. If this option is disabled or if the ADSP record uses a syntax unknown to MDaemon, then the message will be treated as if the domain signs only some of its

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

messages.

**See:**

**DomainKeys Identified Mail** 284
**DKIM Verification** 285
**DKIM Signing** 289

### 5.4.2.4 Message Certification

Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. Consequently, when this certifying entity is one whom a receiving email server trusts, messages sent from a domain who is vouched for by that entity can be viewed with less suspicion. Thus the receiving server can be reasonably assured that the sending domain adheres to a set of good email practices and doesn't send spam or other problematic messages. Certification is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It also helps lower the resources required to process each message.

MDaemon Pro supports Message Certification by including the world's first commercial implementation of a new Internet mail protocol called "Vouch-By-Reference" (VBR), which Alt-N Technologies is working to help create and expand through its participation in the Domain Assurance Council (DAC). VBR provides the mechanism through which Certification Service Providers (CSP) or "certifiers" vouch for the good email practices of specific domains.

## Certifying Incoming Messages

It is easy to configure MDaemon's Message Certification feature to check incoming messages. All you have to do is click the *Enable certification of inbound messages* option on the VBR Certification dialog (Security » Security Settings » Sender Authentication » VBR Certification) and include one or more certification providers whom you trust to vouch for incoming email (e.g. `vbr.emailcertification.org`). You can also choose either to exempt certified messages from spam filtering or give their Spam Filter scores a beneficial adjustment.

## Certifying Outgoing Messages

Before you can configure MDaemon to insert certification data into your outgoing messages, you will first need to arrange to have one or more CSPs certify your email. Alt-N Technologies provides a certification service for MDaemon customers. For details, visit: `www.altn.com`.

To configure your MDaemon server to use Message Certification with your outgoing mail, after you have registered with a CSP:

1. Open the VBR Certification dialog: click Security » Security Settings » Sender Authentication » VBR Certification.
2. Click "*Insert certification data into outgoing messages.*"

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

3. Click "*Configure a domain for message certification.*" This opens the Certification Setup dialog.
4. Type the *Domain name* whose outgoing messages will contain the certification data.
5. Use the *Mail type* drop-down list to choose the type of email that your CSP agrees to certify for this domain, or enter a new type if the desired type isn't listed.
6. Enter one or more CSPs who will certify the domain's outbound email. If you have more than one CSP then use a space to separate each one.
7. Click "*OK.*"
8. Configure your server to sign the domain's outgoing messages with DKIM or DK 284, or ensure that they are being sent from an SPF or SIDF 282 approved server. This is necessary in order to guarantee that the message originated from you. A message cannot be certified unless the receiving server can first determine that the message is authentic.

VBR does not require the certified messages to be signed by or transmitted to your CSP. The CSP is not signing or validating specific messages—it is vouching for the domain's good email practices.

For information on the certification services provided by Alt-N Technologies, visit:

http://www.altn.com/email-certification/

For more information on VBR and Message Certification, visit:

http://www.domain-assurance.org/

VBR Specification—Internet-Draft 00:

http://files.altn.com/MDaemon/drafts/draft-hoffman-dac-vbr-00.txt

For more information on DKIM visit:

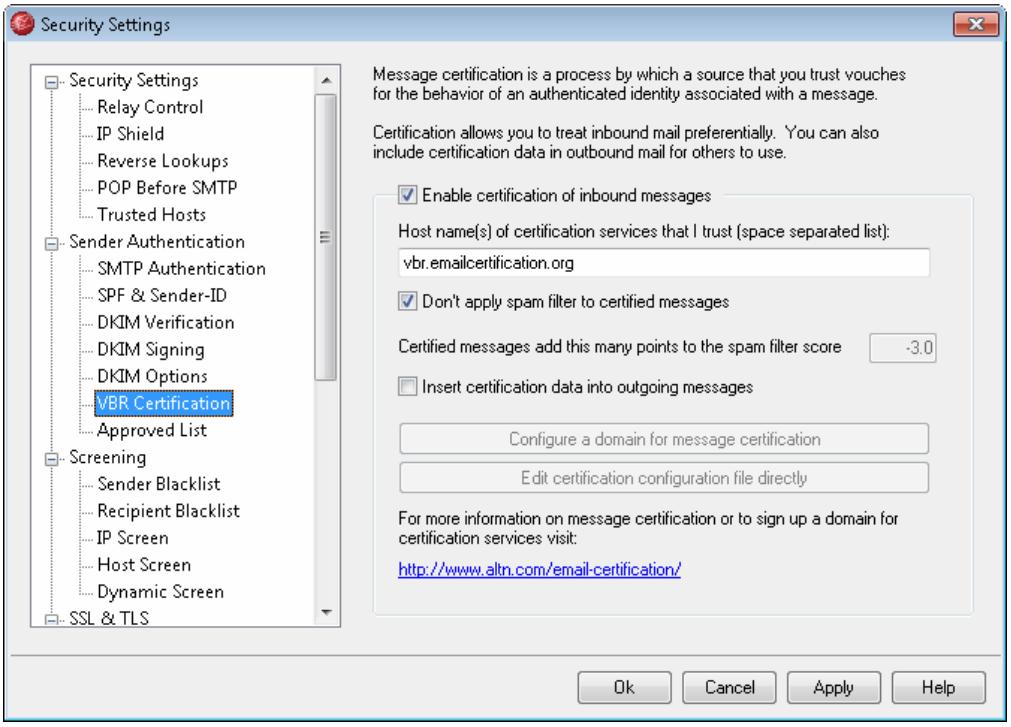
http://www.dkim.org/

**See:**

**VBR Certification** 296

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.2.4.1 VBR Certification




The VBR Certification dialog is located at: Security » Security Settings » Sender Authentication » VBR Certification.

#### Message Certification

**Enable certification of inbound messages**
Click this checkbox to enable certification of inbound messages. When MDaemon receives an inbound message needing certification, it will query the trusted CSP to confirm whether or not the message should actually be considered "certified." If so then the message will either be exempt from spam filtering or have its Spam Filter score adjusted, depending up which option you have selected below.

**Host name(s) of certification services that I trust (space separated list):**
Use this box to enter the host names of the certification services that you trust. If you trust multiple services then separate each one with a space.

**Don't apply spam filter to certified messages**
Choose this option if you wish to exempt certified messages from the Spam Filter.

**Certified messages add this many points to the spam filter score**
If you do not wish to exempt certified messages from spam filtering, use this option to designate the amount by which you wish to adjust the message's Spam Filter score. Ordinarily this should be a negative number so that certified messages will receive a beneficial adjustment. The default setting is "-3.0".

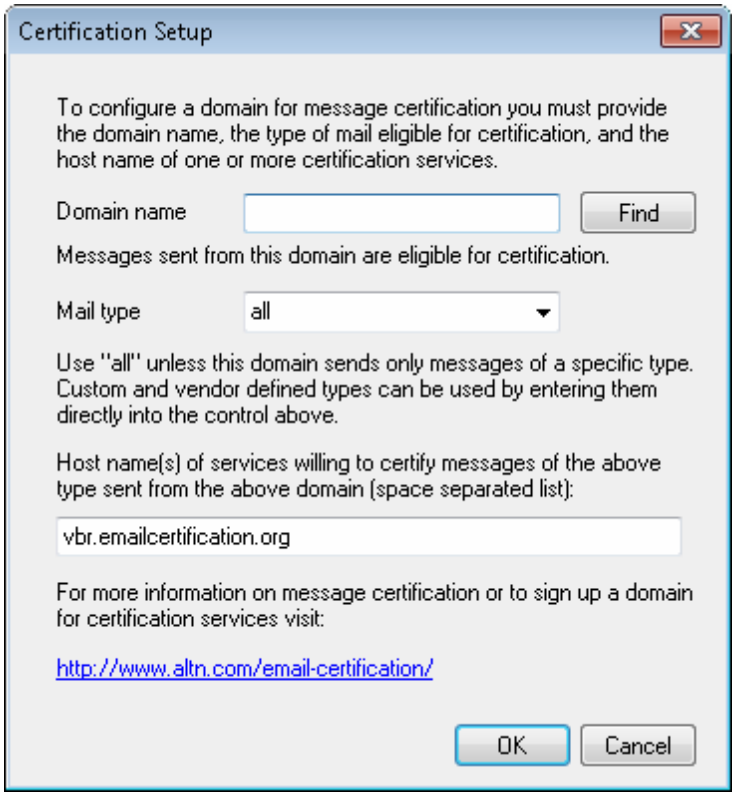
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Insert certification data into outgoing messages**
Click this checkbox to insert the certification data into outgoing messages. Then, click the *Configure a domain for message certification* button to open the Certification Setup dialog to designate the specific domains to be certified and CSPs associated with them.

**Configure a domain for message certification**
After enabling the *Insert certification data into outgoing messages* option above, click this button to open the Certification Setup dialog. On this dialog you will designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

**Edit certification configuration file directly**
After enabling the *Insert certification data into outgoing messages* option above, click this button to open the Vouch-by-Reference (VBR) Configuration File. Any domains that you have configured via the Certification Setup dialog to use VBR will be listed in this file, along with the associated VBR data. You can use this file to edit those entries or manually create new entries.

## Certification Setup




After enabling the *Insert certification data into outgoing messages* option on the Certification dialog, click the *Configure a domain for message certification* button to open the Certification Setup dialog. This dialog is used to designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### Certification Setup

**Domain name**
Use this option to enter the domain whose outbound messages will be certified.

**Find**
If you have previously configured the Message Certification settings for a particular domain, type the *Domain name* and then click this button and that domain's settings will be listed in the Certification Setup dialog's options.

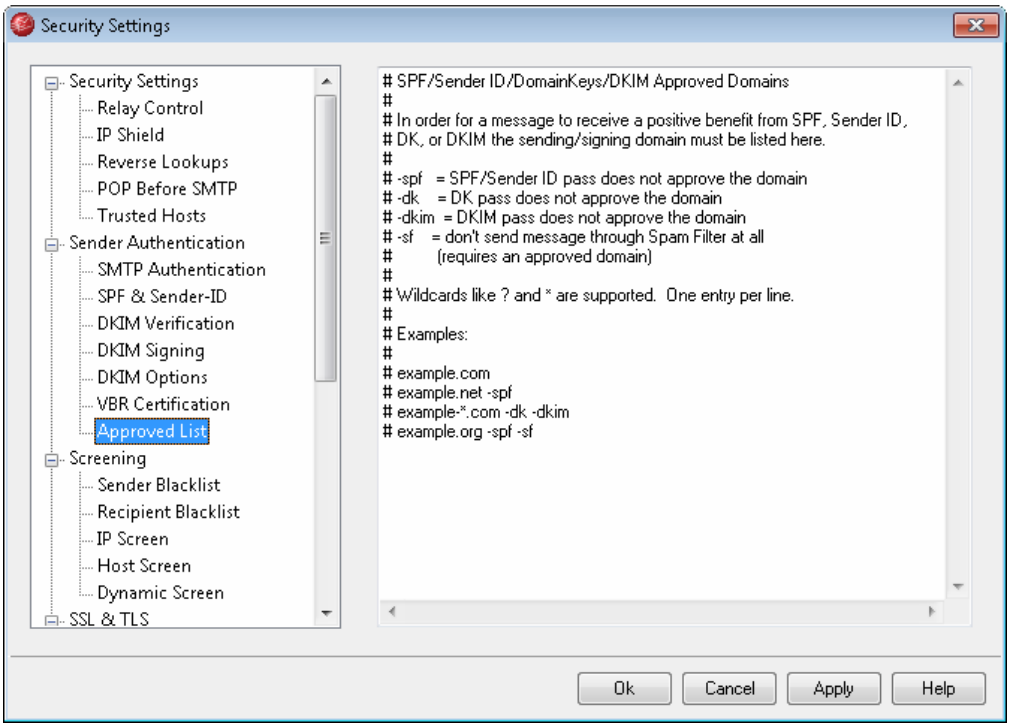
**Mail type**
Use this drop-down list to choose the type of mail that the associated CSP has agreed to certify for this domain. If the type is not listed then you can type it in manually.

**Host names(s) of services...**
Enter the host names of the CSPs who have agreed to certify the domain's outbound messages (for example, `vbr.emailcertification.org`). If you enter more than one CSP then separate each one with a space.

**See:**

**Message Certification** 294

## 5.4.2.5 Approved List




Because some spammers and senders of bulk email have begun using SPF or signing

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

messages with valid DK or DKIM signatures, the fact that a message is signed and verified is no guarantee that you won't consider it to be spam, even though it does ensure that the message originated from a valid source. For this reason, a message's spam score will not be lowered as a result of SPF, Sender ID, DK, or DKIM verification unless the domain taken from the signature is on the Approved List. This is essentially a white list that you can use to designate domains permitted to have their messages' spam scores reduced when those incoming messages are verified.

When a message signed by one of these domains is verified by SPF, Sender ID, DK or DKIM, its spam score will be reduced according to the settings found on the SPF & Sender ID 282 and DKIM Verification 285 screens. You can, however, append any combination of the flags listed below if you wish to prevent one or more of those verification methods from reducing the score. There is also a flag that you can use to prevent verified messages from being passed through the Spam Filter.

-spf Don't lower the spam score for SPF or Sender ID verified messages sent by this domain.

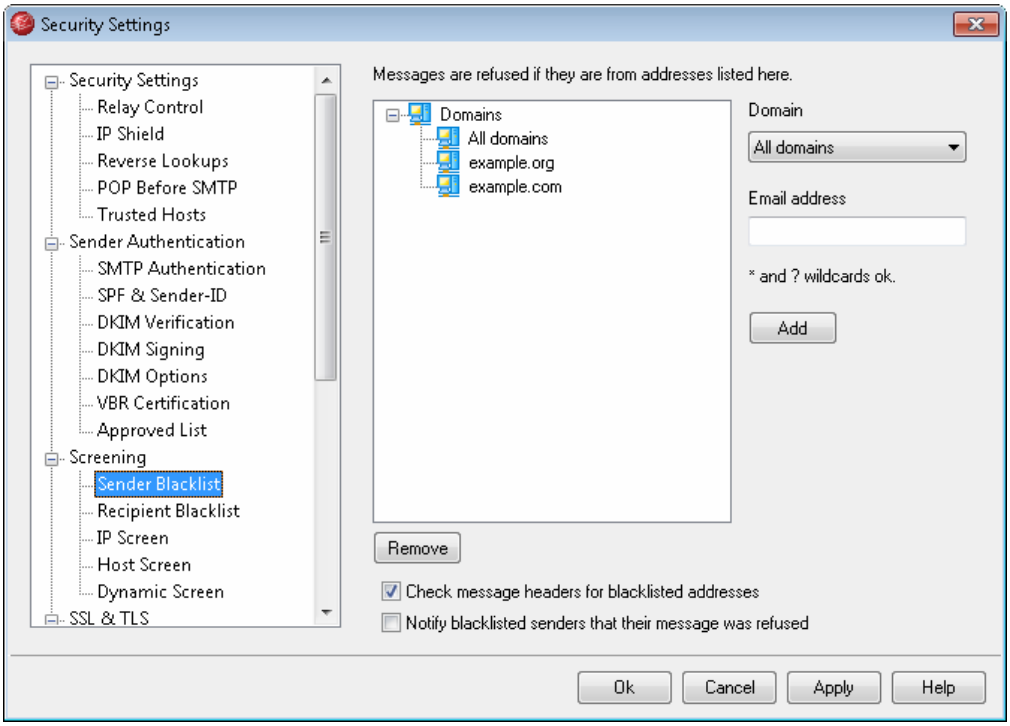
-dk Don't lower the spam score for DK verified messages from this domain.

-dkim Don't lower the spam score for DKIM verified messages from this domain.

-sf Don't process verified messages from this domain through the Spam Filter.

## 5.4.3 Screening

### 5.4.3.1 Sender Blacklist




The Sender Blacklist is located at: Security » Security Settings » Screening. This list

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

contains addresses that are not allowed to send mail traffic through your server. If a message arrives from an address on this list, it will be refused during the SMTP session. This is useful for controlling problem users. Addresses may be blacklisted on a per domain basis or globally (applied to all MDaemon domains).

**Messages are refused if they are from addresses listed here**
This window displays all currently blacklisted addresses, listed by the domain that is blacklisting them.

**Domain**
Choose the domain with which this blacklisted address will be associated. In other words, what domain do you wish to prevent from receiving mail from the specified address? Choose "All Domains" from this list to blacklist the address globally.

**Email address**
Enter the address that you wish to blacklist. Wildcards are accepted, therefore "*@example.net" will suppress any message from any user at "example.net", and "user1@*" will suppress any message from any address beginning with "user1@", regardless of the domain the message is from.

**Add**
Click this button to add the designated address to the black list.

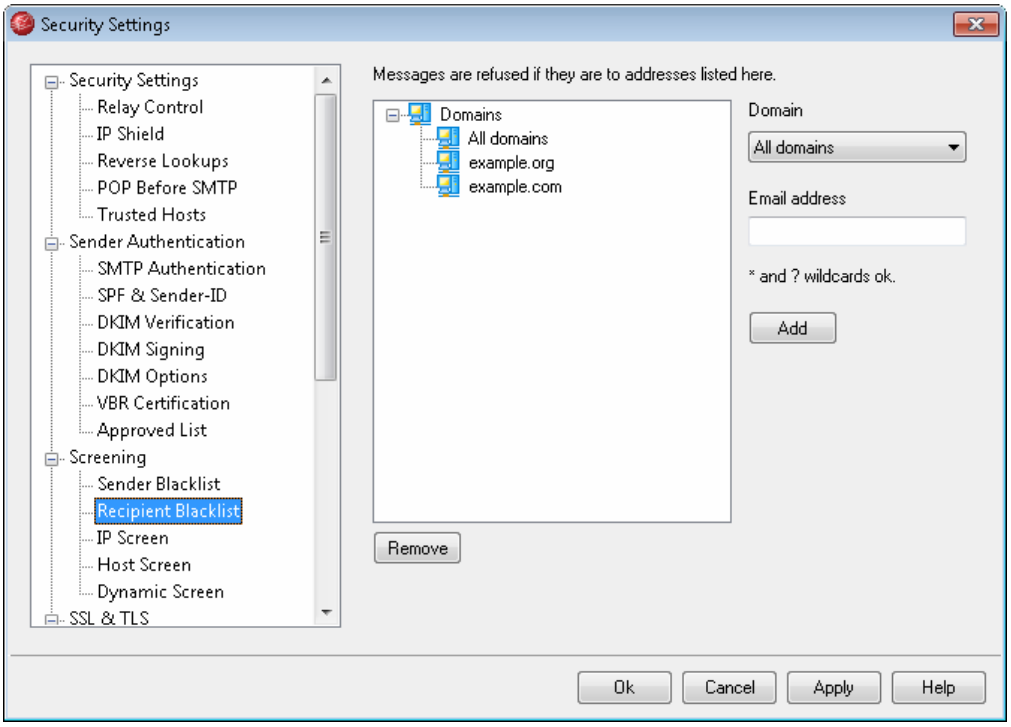
**Remove**
Click this button to remove an entry that you have selected in the list.

**Check message headers for blacklisted senders**
By default, MDaemon applies the blacklist to values taken from the message's From/ Sender header(s) during the SMTP session (after DATA completes). This prevents the message from getting caught later and moved into the bad queue by the MTA thread.

**Notify blacklisted senders that their message was refused**
If selected, a message will be routed back to the blacklisted sender telling him or her that the message was refused.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.3.2 Recipient Blacklist




The Recipient Blacklist is located at: Security » Security Settings » Screening. This list contains email addresses that are not allowed to receive mail through your server. If a message arrives for an address on this list, it will be refused. Addresses may be blacklisted on a per domain basis or globally (applied to all MDaemon domains). The Recipient Blacklist operates on SMTP envelope RCPT data only (not message headers).

**Messages are refused if they are to addresses listed here**
This window displays all currently blacklisted addresses, listed by the domain that is blacklisting them.

**Domain**
Choose the domain with which this blacklisted address will be associated. In other words, what domain do you wish to prevent from receiving mail for the specified address? Choose "All Domains" from this list to blacklist the address globally.

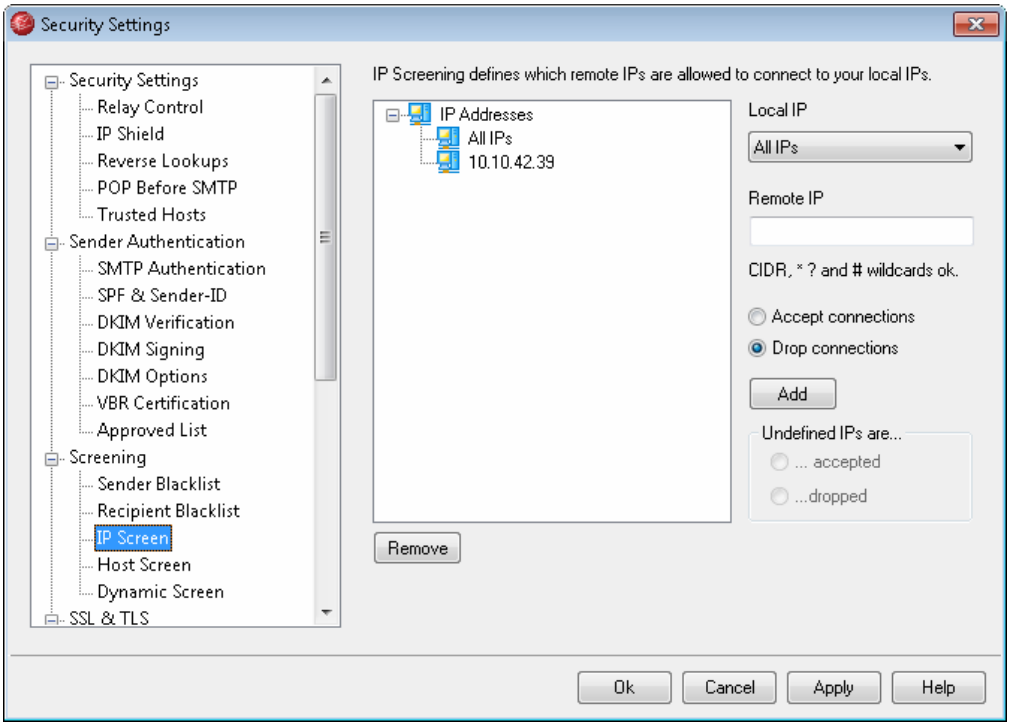
**Email address**
Enter the address that you wish to blacklist. Wildcards are accepted, therefore "*@example.net" will suppress any message for any user at "example.net", and "user1@*" will suppress any message for any address beginning with "user1@", regardless of the domain to which the message is addressed.

**Add**
Click this button to add the designated address to the black list.

**Remove**
Click this button to remove an entry that you have selected in the list.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.3.3 IP Screen




The IP Screen is located at: Security » Security Settings » Screening. The IP Screen is used to define which remote IP addresses will be allowed to connect to your local IP addresses. You may specify a list of IP addresses and configure the server to allow only connections from those on the list, or you can configure it to abort any connection attempt from an IP address on the list. The remote IP addresses you place on the IP Screen can be associated with either all of you local IP addresses or for individual IPs. CIDR notation and the wildcards *, #, and ? are allowed.

For example:

| | |
|---|---|
| *.*.*.* | Matches to any IP address |
| #.#.#.# | Matches to any IP address |
| 192.*.*.* | Matches to any IP that begins with 192 |
| 192.168.*.239 | Matches to IP addresses from 192.168.0.239 to 192.168.255.239 |
| 192.168.0.1?? | Matches to IP addresses from 192.168.0.100 to 192.168.0.199 |

**Local IP**
Choose from the drop-down list either "All IP's" or the local IP to which you wish to apply the screen.

**Remote IP**
Enter the remote IP address that you wish to add to the list, associated with the Local IP designated above.

**Accept connections**
Selecting this option means that the specified remote IP addresses will be allowed

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

to connect to the associated local IP address.

**Drop connections**
Selecting this option means that the specified remote IP addresses will NOT be allowed to connect to the associated local IP address. The connection will be refused or dropped.

**Add**
When you have finished entering the information in the options above, click this button to add the entry to the list.

**Remove**
Select an entry and then click this button to remove it from the list.

### Undefined IPs are...

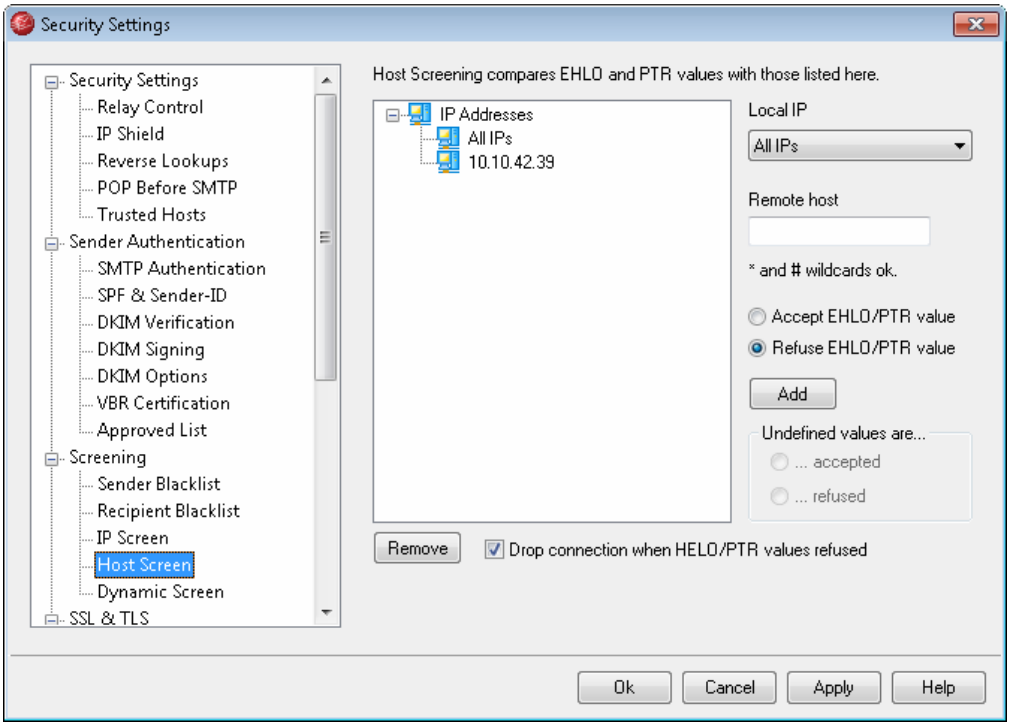
**...accepted**
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be accepted.

**...dropped**
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be dropped, or refused.

The IP Screen will never block trusted IPs 279 or local IPs.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.3.4 Host Screen




The Host Screen is located at: Security » Security Settings » Screening. The Host Screen is used to define which remote hosts will be allowed to connect to your local IP addresses. You may specify a list of hosts and configure the server to allow only connections from those hosts, or you can configure it to refuse connections from the listed hosts. Host screening compares the EHLO and PTR values determined during the SMTP session with the values specified here.

**Local IP**
Use this drop-down list to choose the local IP address to which this Host Screen entry will apply. Choose "All IPs" if you wish it to apply to all of your local IP addresses.

**Remote host**
Enter the remote host that you wish to add to the list, associated with the Local IP designated above.

**Accept EHLO/PTR value**
Selecting this option means that the specified remote host will be allowed to connect to the associated local IP address.

**Refuse EHLO/PTR value**
Selecting this option means that the specified remote host will NOT be allowed to connect to the associated local IP address. The connection will be refused, or it will be dropped if you have enabled "*Drop connection when HELO/PTR values refused*" below).

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Add**
When you have finished entering the information in the options above, click this button to add the entry to the list.

**Remove**
Select an entry and then click this button to remove it from the list.

### Undefined hosts are...

**...accepted**
When this option is chosen, connections from any host not specifically defined on the Host Screen will be accepted.

**...refused**
When this option is chosen, connections from any host not specifically defined on the Host Screen will be refused.

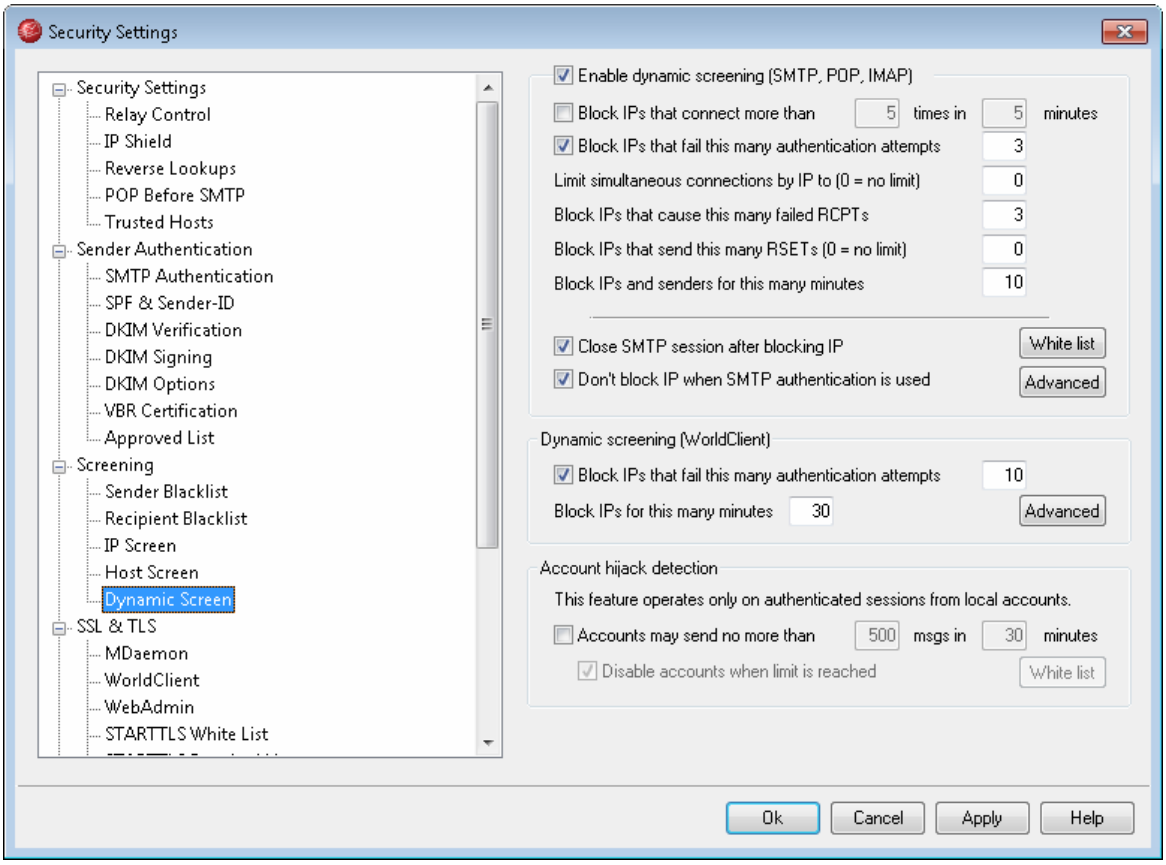
The Host Screen will never block trusted 279 or local hosts.

### Drop connection when HELO/PTR values refused

Check this box if you want the connection to be dropped when an HELO/PTR value is refused by the Host Screen.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.3.5 Dynamic Screen




Using the Dynamic Screening features, MDaemon can track the behavior of sending servers to identify suspicious activity and then respond accordingly. For example, you can temporarily block an IP address from future connections to your server once a specified number of "unknown recipient" errors occur during the mail connection from that IP address. You can also block senders that connect to your server more than a specified number of times in a specified number of minutes, and senders that fail authentication attempts more than a designated number of times.

When a sender is blocked, it is not permanent. The sender's IP address will be blocked for the number of minutes that you have specified on this dialog. Blocked addresses are contained in the `DynamicScreen.dat` file. It contains a list of the blocked IP addresses and the length of time each will be blocked. This file is memory resident and can be changed from the *Advanced* button. If you wish to edit or add the IP addresses manually using a text editor, you should create the `DynamicScreenUpd.sem` Semaphore File[512] and place it in MDaemon's `\APP\` folder rather than editing the `DynamicScreen.dat` file directly.

The "Dynamic screening (WorldClient)" section provides options that allow you to screen WorldClient connections.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## Dynamic Screening

**Enable dynamic screening (SMTP, POP, IMAP)**
Click this check box to enable dynamic screening. This option screens SMTP, POP3, and IMAP connections.

**Block IPs that connect more than [X] times in [X] minutes**
Click this check box if you wish to temporarily block IP addresses that connect to your server an excessive number of times in a limited time period. Specify the number of minutes and the number of connections allowed in that period.

**Block IPs that fail this many authentication attempts**
Use this option if you wish to temporarily block IPs that fail an authentication attempt a specified number of times. This can help prevent attempts to "hack" a user account and falsely authenticate a session. This option monitors SMTP, POP3, and IMAP connections.

**Limit simultaneous connections by IP to (0 = no limit)**
This is the maximum number of simultaneous connections allowed from a single IP address before it will be blocked. Use "0" if you do not wish to set a limit.

**Block IPs that cause this many failed RCPTs**
When an IP address causes this number of "Recipient unknown" errors during a mail session it will be automatically blocked for the number of minutes specified in the *Block IPs for this many minutes* option below. Frequent "Recipient unknown" errors are often a clue that the sender is a spammer, since spammers commonly attempt to send messages to outdated or incorrect addresses.

**Block IPs that send this many RSETs (0 = no limit)**
Use this option if you wish to block any IP address that issues the designated number of RSET commands. Use "0" if you do not wish to set a limit. There is a similar option on the Servers 46 screen under Default Domains & Servers that can be used to set a hard limit on the allowed number of RSET commands.

**Block IPs and senders for this many minutes**
When an IP address or sender is automatically blocked, this is the number of minutes the block will last. When the block expires the IP or sender will be able to send to you again normally. This feature prevents you from accidentally blocking a valid IP address or sender permanently.

---

**Close SMTP session after blocking IP**
Enabling this option causes MDaemon to close the SMTP session after the IP address is blocked.

**Don't block IP when when SMTP authentication is used**
Click this checkbox if you want senders who authenticate their mail sessions before sending to be exempt from Dynamic Screening.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**White list**
Click this button to open the Tarpit/Dynamic Screening white list. IP addresses listed there are exempt from tarpitting and dynamic screening.

**Advanced**
Click this button to open the `DynamicScreen.dat` block list. This lists all IP addresses that have been blocked by Dynamic Screening. You can manually add IP addresses and the number of minutes to block them by listing them one entry per line in the form: `IP_address<space>Minutes`. For example, `192.0.2.0 60`.

### Dynamic Screening (WorldClient)

**Block IPs that fail this many authentication attempts**
Use this option if you wish to temporarily block IP addresses that fail a WorldClient authentication attempt a specified number of times. This can help prevent attempts to "hack" a user account and falsely authenticate a session. This option monitors only WorldClient connections.

**Block IPs for this many minutes**
When an IP address is automatically blocked, this is the number of minutes the block will last. When the block expires the IP address will be able to connect to you again normally. This feature prevents you from accidentally blocking a valid IP address permanently.

**Advanced**
Click this button to open the Dynamic Screen's WorldClient block list. This lists all IP addresses that have been blocked from connecting to WorldClient. You can manually add IP addresses and the number of minutes to block them by listing them one entry per line in the form: `IP_address<space>Minutes`. For example, `192.0.2.0 60`.

### Account Hijack Detection

The options in this section can be used to detect a possibly hijacked MDaemon account and automatically prevent it from sending messages through your server. For example, if a spammer somehow obtained an account's email address and password then this feature could prevent the spammer from using the account to send bulk junk e-mail through your system. You can designate a maximum number of messages that may be sent by an account in a given number of minutes, and optionally cause an account to be disabled if it reaches that limit. There is also a *White List* that can be used to exempt certain addresses from this restriction.

Account Hijack Detection only applies to local accounts over authenticated sessions, and the Postmaster account is automatically exempt.

**Accounts may send no more than [xx] msgs in [xx] minutes**
Use this option if you wish to prevent MDaemon accounts from sending more than the specified number of messages in the designated number of minutes. If an account attempts to send more than the allowable number of messages then MDaemon will not drop the connection but it will reject the over-the-limit messages

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

with a 452 error until the time-limit expires. Then it will again accept messages from the account.

**Disable accounts when limit is reached**
Check this box if you wish to disable accounts that attempt to send more than the allowable number of messages. When this happens, the server sends a 552 error, the connection is dropped, and the account is immediately disabled. The disabled account will no longer be able send mail or check its mail, but MDaemon will still accept incoming mail for the account. Finally, when the account is disabled an email is then sent to the postmaster about the account. If the postmaster wishes to re-enable the account that he can simply reply to the message.

**White List**
Use the *White List* to designate any addresses that you wish to exempt from Account Hijack Detection. Wildcards are permitted. For example, "newsletters@example.com" would exempt example.com's "newsletters" MDaemon account, while "*@newsletters.example.com" would exempt all MDaemon accounts belonging to the newsletters.example.com domain. The Postmaster account is automatically exempt from Account Hijack Detection.

### 5.4.4 SSL & TLS

MDaemon supports the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol for SMTP, POP, and IMAP, and for WorldClient's web server. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client Internet communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connection. Further, because SSL is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting browser's SSL capabilities when connecting to WorldClient.

If you are connecting to the standard mail ports via a mail client instead of using WorldClient, MDaemon supports the STARTTLS extension over TLS for SMTP and IMAP, and the STLS extension for POP3. However, you must first have your client configured to use SSL, and it must support those extensions—not all mail clients support them.

Finally, you can also dedicate specific ports for SSL connections. This isn't required but can provide a further level of accessibility for clients that do not support certain SSL extensions. For example, some versions of Microsoft Outlook Express don't support STARTTLS for IMAP over the default mail port, but do support connections to dedicated SSL ports.

The options for enabling and configuring SSL are located under the SSL & TLS section of the Security Settings dialog at: Security » Security Settings » SSL & TLS. The SSL port settings for SMTP, POP3, and IMAP are located on the Ports 49 screen at: Setup » Default Domain/Servers.

For information on creating and using SSL Certificates, see:

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Creating & Using SSL Certificates** 320

—

The TLS/SSL protocol is addressed in RFC-2246, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2246.txt

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

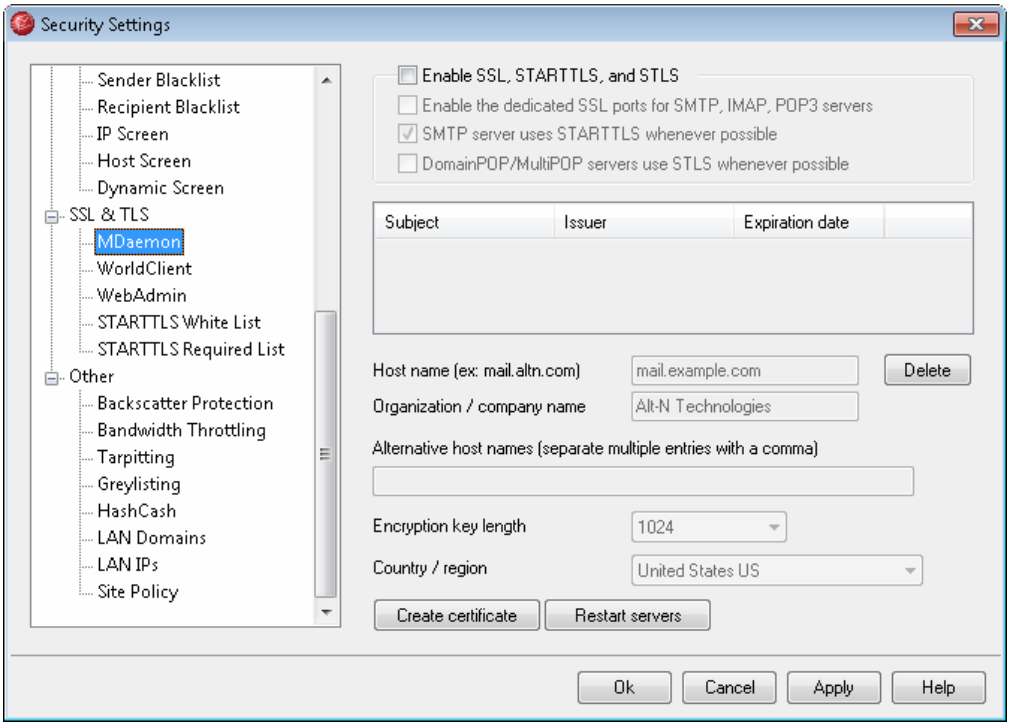
Using TLS with the IMAP and POP3 protocols is addressed in RFC-2595, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2595.txt

**See:**

**SSL & TLS » MDaemon** 310
**SSL & TLS » WorldClient** 313
**SSL & TLS » WebAdmin** 316

### 5.4.4.1 MDaemon




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Enable SSL, STARTTLS, and STLS**
Click this check box to activate support for the SSL/TLS protocol and the STARTTLS and STLS extensions. Then, choose the certificate that you want to use from the list below.

**Enable the dedicated SSL ports for SMTP, IMAP, POP3 servers**
Click this option if you want to make available the dedicated SSL ports specified on Ports 49 under Default Domains & Servers. This will not affect clients using STARTTLS and STLS on the default mail ports — it merely provides an additional level of support for SSL.

**SMTP server uses STARTTLS whenever possible**
Click this option if you want MDaemon to attempt to use the STARTTLS extension for every SMTP message it sends. If a server to which MDaemon is connecting doesn't support STARTTLS then the message will be delivered normally without using SSL. Use the White List 319 in this section if you wish to prevent the use of STARTTLS for certain domains.

**DomainPOP/MultiPOP servers use STLS whenever possible**
Check this box if you want the DomainPOP and MultiPOP servers to use the STLS extension whenever possible.

## Certificate List

This box displays your SSL certificates. Single-click a certificate in this list to designate it as the certificate that you wish the mail servers to use. Double-click a certificate to open it in the Certificate dialog on which you can review its details.

MDaemon does not support different certificates for multiple domains. All mail domains must share a single certificate. If you have more than one domain then enter those domain names under the option, *Alternative host names (separate multiple entries with a comma)* outlined below.

**Delete**
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

The following controls are used to create certificates. To edit any certificate, double-click its entry in the list above.

**Host name**
Enter the host name to which your users will connect (for example, "mail.example.com").

**Organization/company name**
Enter the organization or company that "owns" the certificate here.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Alternative host names (separate multiple entries with a comma)**
MDaemon does not support separate certificates for multiple domains — all domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

**Encryption key length**
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

**Country/region**
Choose the country or region in which your server resides.

**Create Certificate**
After entering the information into the above controls, click this button to create your certificate.

**Restart Servers**
Click to restart the SMTP/IMAP/POP servers. The servers must be restarted when a certificate changes.

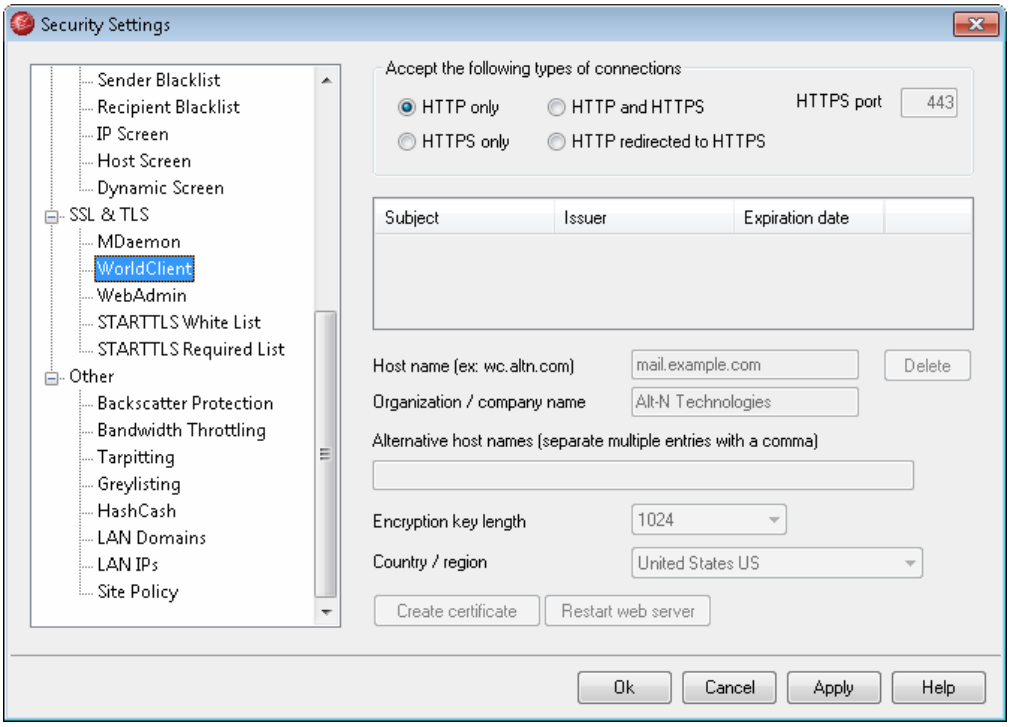
---

**See:**

**SSL & TLS** 309
**Creating and Using SSL Certificates** 320

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.4.2 WorldClient




MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WorldClient to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » WorldClient (web mail)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WorldClient".

For more information on the SSL protocol and Certificates, see: SSL & TLS 309.

This screen only applies to WorldClient when using MDaemon's built-in web server. If you configure WorldClient to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

**Accept the following types of connections**

**HTTP only**
Choose this option if you do not wish to allow any HTTPS connections to

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

WorldClient. Only HTTP connections will be accepted.

**HTTP and HTTPS**
Choose this option if you want to enable SSL support within WorldClient, but do not wish to force your WorldClient users to use HTTPS. WorldClient will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the WorldClient TCP port designated on the Web Server 116 screen of WorldClient (web mail).

**HTTPS only**
Choose this option if you wish to require HTTPS when connecting to WorldClient. WorldClient will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

**HTTP redirects to HTTPS**
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

**HTTPS port**
This is the TCP port that WorldClient will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WorldClient's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WorldClient port that is designated on the Web Server 116 screen of WorldClient (web mail). If you are still allowing HTTP connections to WorldClient then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

## Certificates

This box displays your SSL certificates. Single-click a certificate in this list to designate it as the certificate that you wish WorldClient to use. Double-click a certificate to open it in the Certificate dialog to review its details or edit it.

MDaemon does not support multiple certificates for WorldClient. All WorldClient domains must share a single certificate. If you have more than one WorldClient domain then enter those domain names (and any others that you wish to use to access WorldClient) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

**Delete**
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Host name**
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

**Organization/company name**
Enter the organization or company that "owns" the certificate here.

**Alternative host names (separate multiple entries with a comma)**
MDaemon does not support multiple certificates — all WorldClient domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

**Encryption key length**
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

**Country/region**
Choose the country or region in which your server resides.

**Create Certificate**
After entering the information into the above controls, click this button to create your certificate.

**Restart web server**
Click this button to restart the web server. The web server must be started before new certificates will be used.

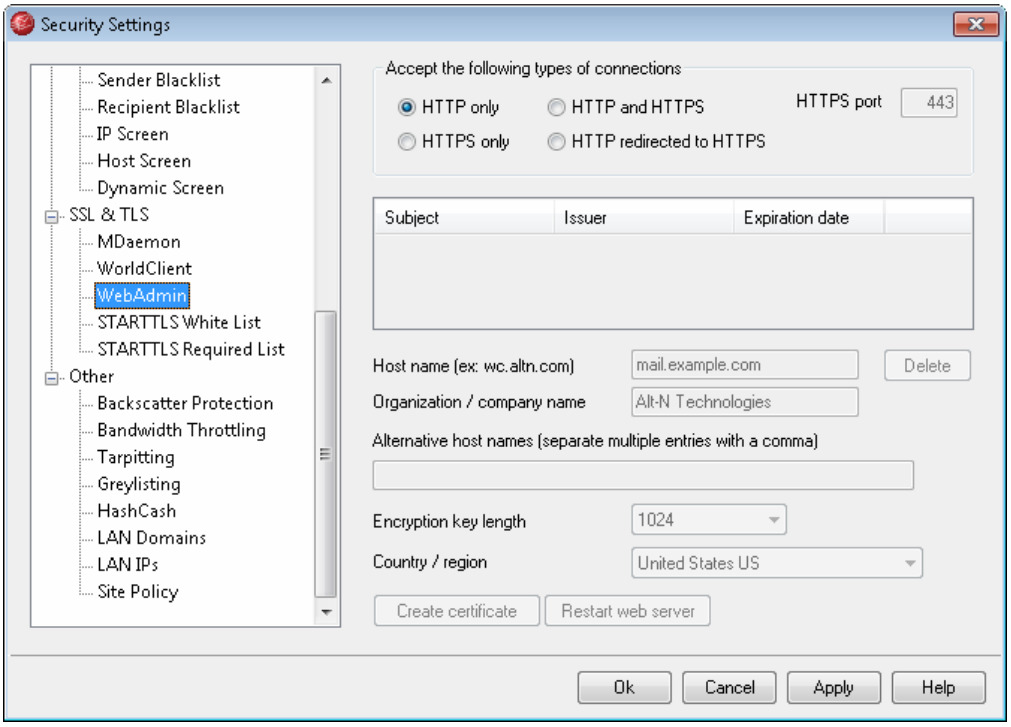
---

**See:**

**SSL & TLS** 309
**Creating and Using SSL Certificates** 320

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.4.3 WebAdmin




MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring WebAdmin to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » WebAdmin (web configuration)". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » WebAdmin".

For more information on the SSL protocol and Certificates, see: **SSL & TLS** 309.

This screen only applies to WebAdmin when using MDaemon's built-in web server. If you configure WebAdmin to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

#### Accept the following types of connections

**HTTP only**
Choose this option if you do not wish to allow any HTTPS connections to WebAdmin.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Only HTTP connections will be accepted.

**HTTP and HTTPS**
Choose this option if you want to enable SSL support within WebAdmin, but do not wish to force your WebAdmin users to use HTTPS. WebAdmin will listen for connections on the *HTTPS port* designated below, but it will still respond to normal http connections on the WebAdmin TCP port designated on the Web Server 134 screen of WebAdmin (web configuration).

**HTTPS only**
Choose this option if you wish to require HTTPS when connecting to WebAdmin. WebAdmin will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

**HTTP redirects to HTTPS**
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

**HTTPS port**
This is the TCP port that WebAdmin will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in WebAdmin's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the WebAdmin port that is designated on the Web Server 134 screen of WebAdmin (web configuration). If you are still allowing HTTP connections to WebAdmin then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

## Certificates

This box displays your SSL certificates. Single-click a certificate in this list to designate it as the certificate that you wish WebAdmin to use. Double-click a certificate to open it in the Certificate dialog to review its details or edit it.

MDaemon does not support multiple certificates for WebAdmin. All domains must share a single certificate. If you have more than one domain then enter those domain names (and any others that you wish to use to access WebAdmin) into the option called "*Alternative host names (separate multiple entries with a comma)*" outlined below.

**Delete**
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Host name**
When creating a certificate, enter the host name to which your users will connect (for example, "wa.example.com").

**Organization/company name**
Enter the organization or company that "owns" the certificate here.

**Alternative host names (separate multiple entries with a comma)**
MDaemon does not support multiple certificates — all domains must share a single certificate. If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

**Encryption key length**
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

**Country/region**
Choose the country or region in which your server resides.

**Create Certificate**
After entering the information into the above controls, click this button to create your certificate.

**Restart web server**
Click this button to restart the web server. The web server must be started before new certificates will be used.

---

**For more information on SSL and Certificates, see:**

**Running WebAdmin under IIS** 138
**SSL and Certificates** 309
**Creating and Using SSL Certificates** 320

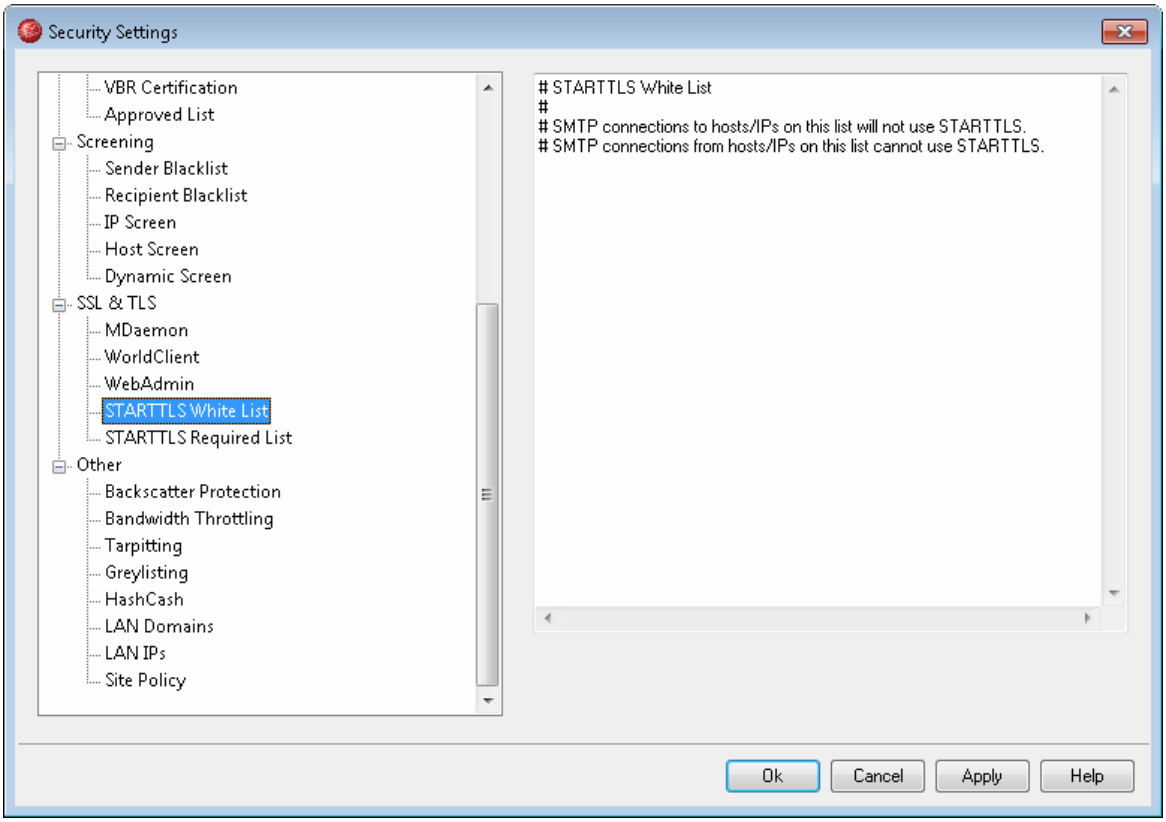
---

**For more information on WebAdmin, see:**

**Remote Configuration** 132
**WebAdmin » Web Server** 134
**Web Access Defaults** 387
**Account Editor » Web** 346

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.4.4 STARTTLS White List



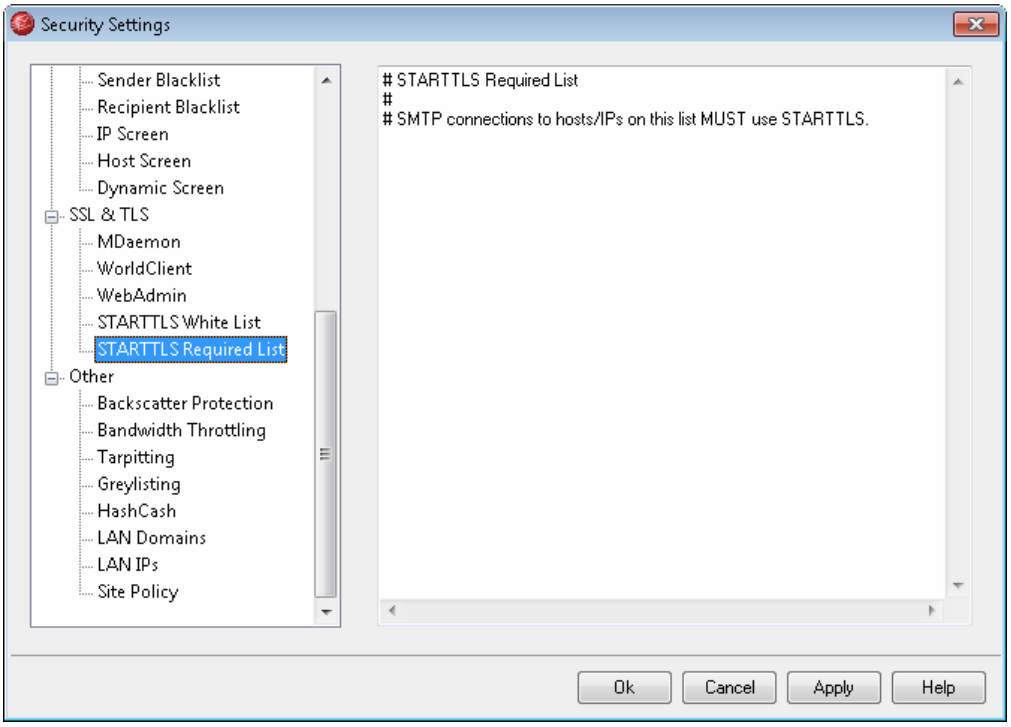

Use this white list to prevent the use of STARTTLS when sending or receiving mail to or from certain hosts or IP addresses.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.4.5 STARTTLS Required List




Use this screen to specify hosts and IP addresses that require the use of the STARTTLS extension in order to receive mail from your server.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

### 5.4.4.6 Creating and Using SSL Certificates

When using the SSL & TLS dialog to create certificates, MDaemon generates certificates that are self-signed. In other words, the issuer of the certificate, or Certificate Authority (CA), is the same as the owner of the certificate. This is perfectly valid and allowed, but because the CA won't already be listed in yours users' lists of trusted CAs, whenever they connect to WorldClient or WebAdmin's HTTPS URL they will be asked whether or not they wish to proceed to the site and/or install the certificate. Once they agree to install the certificate and trust your WorldClient's domain as a valid CA they will no longer have to see the security alert message when connecting to WorldClient or WebAdmin.

When connecting to MDaemon via a mail client such as Microsoft Outlook, however, they will not be given the option to install the certificate. They will be allowed to choose whether or not they wish to continue using the certificate temporarily, even though it isn't validated. Each time they start their mail client and connect to the server, they will have to choose to continue using the non-validated certificate. To avoid this you should export your certificate and distribute it to your users via email or

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

some other means. Then, they can manually install and trust your certificate to avoid future warning messages.

## Creating a Certificate

To create a certificate from within MDaemon:

1. Move to the SSL & TLS dialog within MDaemon (click Security » Security Settings » SSL & TLS » MDaemon).
2. Check the box labeled, "*Enable SSL, STARTTLS, and STLS*".
3. In the text box labeled, "*Host name*", enter the domain to which the certificate belongs (for example, "`mail.example.com`").
4. Type the name of the organization or company that owns the certificate into the text box labeled, "*Organization/company name*".
5. In "*Alternative host names...*", type all other domain names that your users will be using to access your server (for example, "`*.example.com`", "`example.com`", "`mail.altn.com`", and so on).
6. Choose a length for the encryption key from the drop-down list box.
7. Choose the Country/region where your server resides.
8. Click Create certificate.

## Using Certificates Issued by a Third-party CA

If you have purchased or otherwise generated a certificate from some source other than MDaemon, you can still use that certificate by using the Microsoft Management Console to import it into the certificate store that MDaemon uses. To do so in Windows XP:

1. On your Windows toolbar, click **Start » Run...** and then type "**mmc /a**" into the text box.
2. Click **OK**.
3. In the Microsoft Management Console, click **File » Add/Remove Snap-in...** on the menu bar (or press **Ctrl+M** on your keyboard).
4. On the Standalone tab, click **Add...**
5. On the *Add Standalone Snap-in* dialog, click **Certificates**, and then click **Add**.
6. On the *Certificates snap-in* dialog, choose **Computer account**, and then click **Next**.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

7. On the *Select Computer* dialog, choose **Local computer**, and then click **Finish**.
8. Click **Close**, and click **OK**.
9. Under *Certificates (Local Computer)* in the left pane, if the certificate that you are importing is self-signed, click **Trusted Root Certification Authorities** and then **Certificates**. If it is not self-signed then click **Personal**.
10. On the menu bar, click **Action** » **All Tasks** » **Import...**, and click **Next**.
11. Enter the file path to the certificate that you wish to import (using the Browse button if necessary), and click **Next**.
12. Click **Next**, and click **Finish**.

MDaemon will only display certificates that have private keys using the Personal Information Exchange format (PKCS #12). If your imported certificate does not appear in the list then you may need to import a `*.PEM` file, which contains both a certificate key and private key. Importing this file using the same process outlined above will convert it to the PKCS #12 format.

**See:**

**SSL & TLS** 309

## 5.4.5 Other

### 5.4.5.1 Backscatter Protection - Overview

## Backscatter

"Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a "Return-Path" address that is forged. Consequently, when one of these messages is rejected by the recipient's server, or if the recipient has an Autoresponder or "out of office"/vacation message associated with his account, the response message will then be directed to the forged address. This can lead to huge numbers of bogus Delivery Status Notifications (DSNs) or auto response messages ending up in your users' mailboxes. Further, spammers and virus authors frequently take advantage of this phenomenon and will sometimes use it to launch Denial of Service (DoS) attacks against email servers, causing a flood of invalid emails to arrive from servers located all over the world.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## MDaemon's Solution

To combat backscatter, MDaemon contains a feature called Backscatter Protection (BP). BP can help to ensure that only legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the "Return-Path" address of your users' outgoing messages. Then, when one of these messages encounters a delivery problem and is bounced back, or when an auto-reply is received with a "`mailer-daemon@...`" or `NULL` reverse path, MDaemon will see the special code and know that it is a genuine automated reply to a message that was sent by one of your accounts. If the address doesn't contain the special code, or if the code is more than seven days old, it will be logged by MDaemon and can be rejected.

Backscatter Protection 323 is located under MDaemon's Security menu at: `Security » Security Settings » Other » Backscatter Protection`.

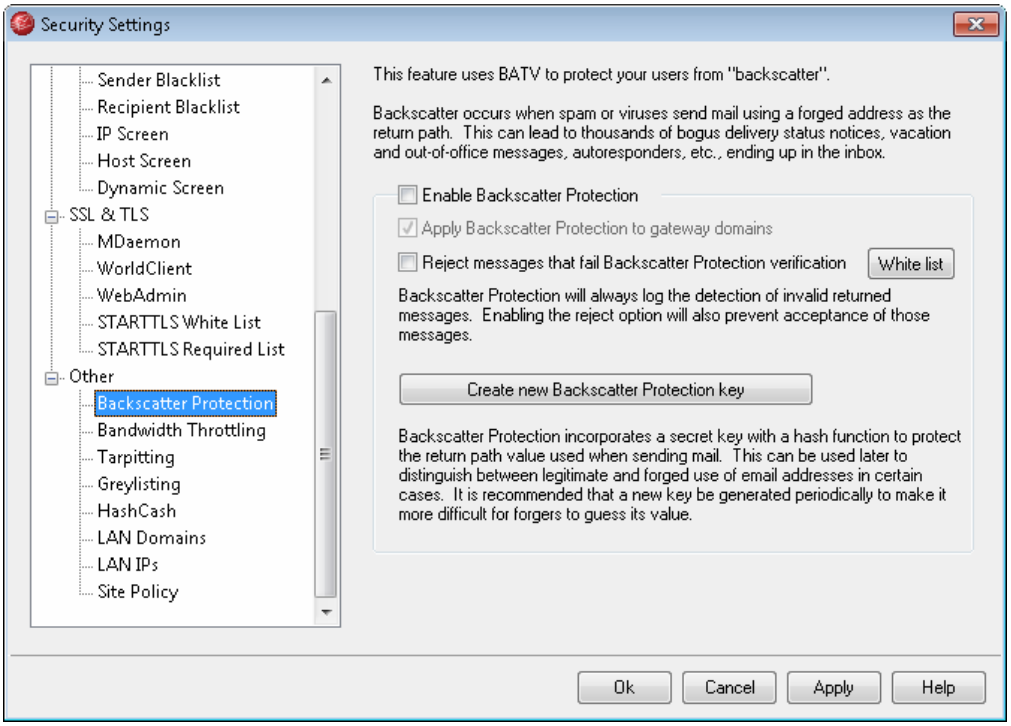
Backscatter Protection is an implementation of Bounce Address Tag Validation (BATV). For more on BATV, visit:

`http://www.mipassoc.org/batv/`

**See:**

**Backscatter Protection** 323

### 5.4.5.1.1 Backscatter Protection




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## Backscatter Protection

**Enable Backscatter Protection**
Click this checkbox if you wish to insert a special Backscatter Protection code into each outgoing message's "Return-Path" address. MDaemon will generate this special code by using the private key found in the `rsa.private` file located in MDaemon's `PEM\_batv\` folder, and the code will be valid for seven days. Any incoming DSNs or other auto-response messages (with a "`mailer-daemon@...`" or `NULL` reverse path) must have a valid, non-expired BP code or they will fail BP verification.

If you disable this option, MDaemon will not insert the special Backscatter Protection code into outgoing messages. It will, however, continue to check incoming DSNs and auto-response messages to ensure that any incoming message with a valid code is not rejected by mistake.

**Apply Backscatter Protection to gateway domains**
When Backscatter Protection is enabled, click this option if you also wish to apply it to domains for which MDaemon is acting as a gateway or backup server (see Domain Gateways 458).

**Reject messages that fail Backscatter Protection verification**
Click this checkbox if you wish to reject DSNs or other auto-response messages that fail BP verification. Messages with a "`mailer-daemon@...`" or `NULL` reverse path will fail if they do not contain the special code or if the code's seven day life-cycle has expired. Because of Backscatter Protection's solid reliability, there are no false positives or "gray areas" — a message is valid or it isn't. For this reason it is safe to configure MDaemon to reject invalid messages, as long as you ensure that all of your accounts' outgoing messages contain the special BP code. In all cases, however, the result of BP verification will be logged into the SMTP-in log file, even when you choose not to reject messages that fail verification. Incoming messages for gateways will not be rejected unless you have checked the *...apply Backscatter Protection to gateway domains* option above.

When you enable Backscatter Protection, you should wait about a week before setting it to reject invalid auto-response messages. This is because during that time you might still receive DSNs or auto-responses to messages that were sent out before BP was activated. If BP were configured to reject invalid message during that time then those legitimate response messages would be rejected by mistake. After a week it should be safe to start rejecting invalid messages. This same warning applies when you create a new BP key and choose to delete the old key immediately instead of allowing it to continue working for another seven days. (see the *Create new Backscatter Protection key* option below).

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**White List**
Click this button to open the Backscatter Protection white list. Use this list to designate any IP addresses or domains that you wish to exempt from Backscatter Protection.

**Create new Backscatter Protection key**
Click this button to generate a new Backscatter Protection key. This key is used by MDaemon to create and then verify the special BP codes that are inserted into messages. The key is located in a file called `rsa.private` in MDaemon's `PEM\_batv\` folder. When the new key is generated, a box will open to inform you that the old key will continue to work for seven more days unless you wish to delete it immediately. In most cases you should click "**No**", electing to allow the key to work for seven more days. If you choose to delete the key immediately then that could cause some incoming messages to fail BP verification, since they would be responses to messages containing the special code generated by the old key.

If you have your email traffic split across multiple servers, you may need to share the key file with all of your other servers or Mail Transfer Agents (MTAs).

**See:**

**Backscatter Protection - Overview** 322

### 5.4.5.2 Bandwidth Throttling - Overview

The Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress — you can set different rates for each of MDaemon's major services on a per-domain basis, including the Domains and Domain Gateways. You can also set limits on local connections by selecting "Local traffic" from a drop down box. This will allow you to create special bandwidth settings that will take effect if the connection is either from or to a local IP address or domain name.

Bandwidth Throttling can be applied on either a per-session or per-service basis. When using the per-session mode, each session will be independently throttled to the associated rate. Thus multiple sessions of the same service type occurring simultaneously could exceed a service's configured value. When configured to throttle bandwidth on a per-service basis, MDaemon will monitor the combined use of all sessions of the same service type and allocate equal fractions of the total bandwidth to each. Multiple sessions will then share the configured maximum bandwidth equally. This will allow you to set a limit on an entire service.

When extending Bandwidth Throttling to a Domain Gateway, it must be handled a bit differently than a normal domain since a Domain Gateway doesn't have a specific IP address associated with it. MDaemon must use the value passed in the RCPT command to determine whether or not an inbound SMTP session is bound for the gateway. If it is, then inbound SMTP bandwidth throttling will be applied. Due to the limitations of

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

SMTP, if even one recipient of a multiple recipient message is destined for a Domain Gateway then the entire session will be throttled.

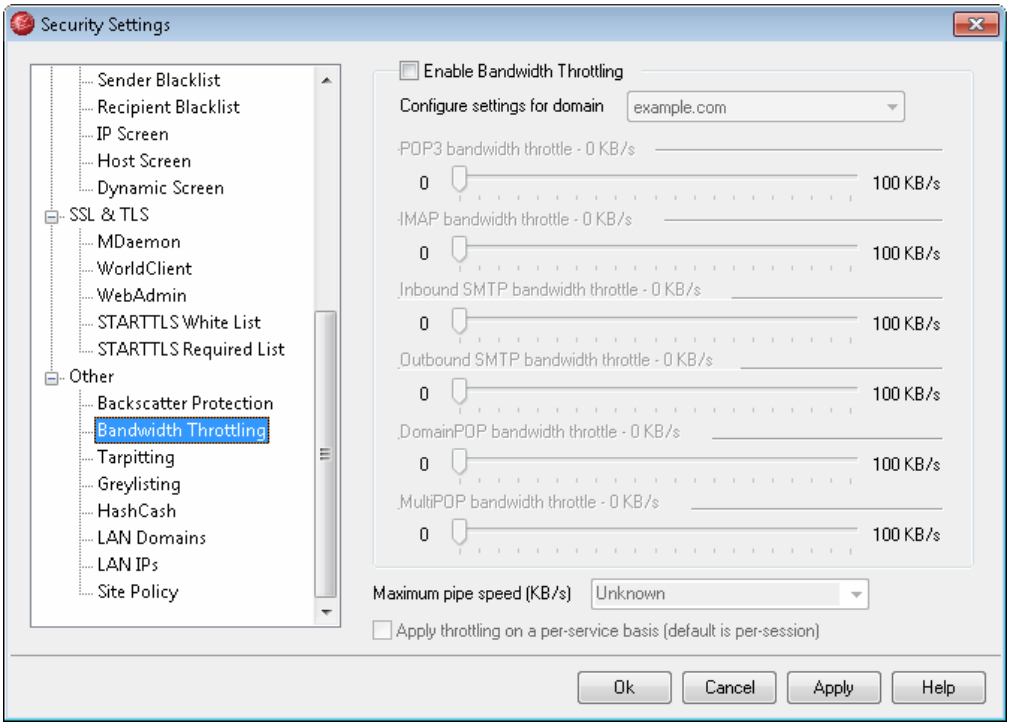
The Bandwidth Throttling system is calibrated in kilobytes per second (KB/s). A value of "0" means that no limit will be applied to the speed at which a session (or service) progresses, thus it will use the maximum amount of available bandwidth. A value of "10", for example, will force MDaemon to deliberately throttle back on the speed of transmission so as to remain at or slightly above 10 KB/s.

Bursts of activity at the beginning of a session can and will exceed the fixed limits. Throttling takes place and becomes more defined as the session progresses.

**See:**

**Bandwidth Throttling** 326
**LAN IPs** 336

### 5.4.5.2.1 Bandwidth Throttling




**Enable Bandwidth Throttling**
Check this box if you wish to activate the Bandwidth Throttling feature.

**Configure settings for domain**
Choose a domain from the drop-down list box and then adjust the options corresponding to the various services to configure bandwidth throttling for the selected domain. A setting of "0" in any particular control means no bandwidth limit is set for that service type. In the drop-down list box, the bottom entry listed is

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*Local traffic*. Setting bandwidth throttling for this option will determine the limits placed on local traffic (i.e. sessions and services occurring on your local LAN rather than externally). The LAN IPs 336 screen can be used for listing IP addresses that should be treated as local.

### Services

**[Service type] bandwidth throttle – XX KB/s**
After selecting a domain from the drop-down list box, adjust these controls to set bandwidth limitations for the selected domain. A setting of "0" means no bandwidth limit is applied to that particular service type. Setting a slider to any number other than "0" will limit the maximum bandwidth to that number of Kilobytes per second for the designated service.

**Maximum pipe speed (KB/s)**
From the drop-down list box, choose the maximum speed of your connection in Kilobytes per second.

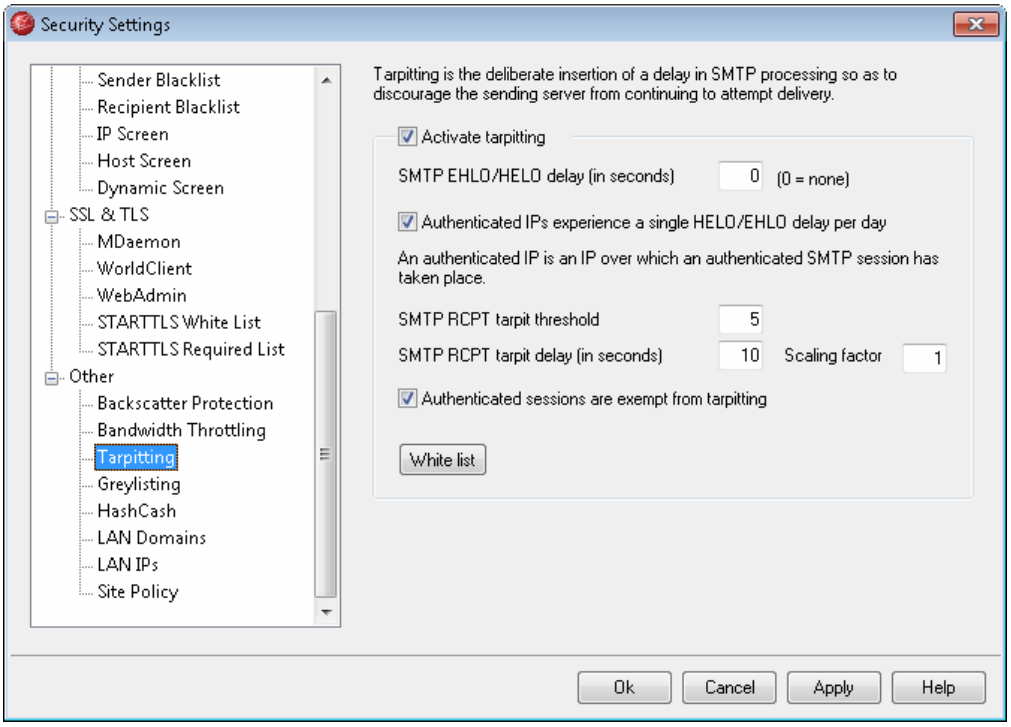
**Apply throttling on a per-service basis (default is per-session)**
Click this checkbox if you want to throttle bandwidth on a per-service basis rather than the default per-session basis. When throttling on a per-service basis, the service's designated amount of bandwidth will be divided equally among all active sessions of the given service type. Thus, the total amount of bandwidth used, for example, by multiple IMAP clients connecting at the same time could never exceed the designated amount regardless of how many clients were connected. If throttling on a per-*session* basis, then no single IMAP session could exceed the designated limit but the total of multiple simultaneous sessions could.

**See:**

**Bandwidth Throttling - Overview** 325

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.5.3 Tarpitting




Tarpitting is located under the Security menu at: Security » Security Settings » Other » Tarpitting.

Tarpitting makes it possible for you to deliberately slow down a connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to use your server to send unsolicited bulk email ("spam"). You can specify the number of RCPT commands allowed before tarpitting begins and the number of seconds to delay the connection each time a subsequent command is received from that host during the connection. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to use your server to do so again in the future.

**Activate tarpitting**
Click this check box to activate MDaemon's tarpitting features.

**SMTP EHLO/HELO delay (in seconds)**
Use this option to delay the server response to EHLO/HELO SMTP commands. Delaying the responses by even as little as ten seconds can potentially save a significant amount of processing time by reducing the amount of spam received. Frequently spammers depend on rapid delivery of their messages and therefore do not wait long for a response to EHLO/HELO commands. With even a small delay, spam tools will sometimes give up and move on rather than wait for a response. Connections on the MSA port (designated on the Ports 49 screen under Default Domain & Servers 40) are always exempt from this delay. The default setting for this option is "0", meaning EHLO/HELO will not be delayed.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Authenticated IPs experience a single EHLO/HELO delay per day**
Click this check box if you wish to limit the EHLO/HELO delay to once per day for authenticated connections from a given IP address. The first message from that IP address will be delayed, but any subsequent messages sent from the same IP address will not.

**SMTP RCPT tarpit threshold**
Specify the number of SMTP `RCPT` commands that you wish to allow for a given host during a mail session before MDaemon will begin tarpitting that host. For example, if this number was set to 10 and a sending host attempted to send a message to 20 addresses (i.e. 20 `RCPT` commands), then MDaemon would allow the first 10 normally and then pause after each subsequent command for the number of seconds specified in the *SMTP RCPT tarpit delay* control below.

**SMTP RCPT tarpit delay (in seconds)**
Once the *SMTP RCPT tarpit threshold* is reached for a host, this is the number of seconds that MDaemon will pause after each subsequent `RCPT` command is received from that host during the mail session.

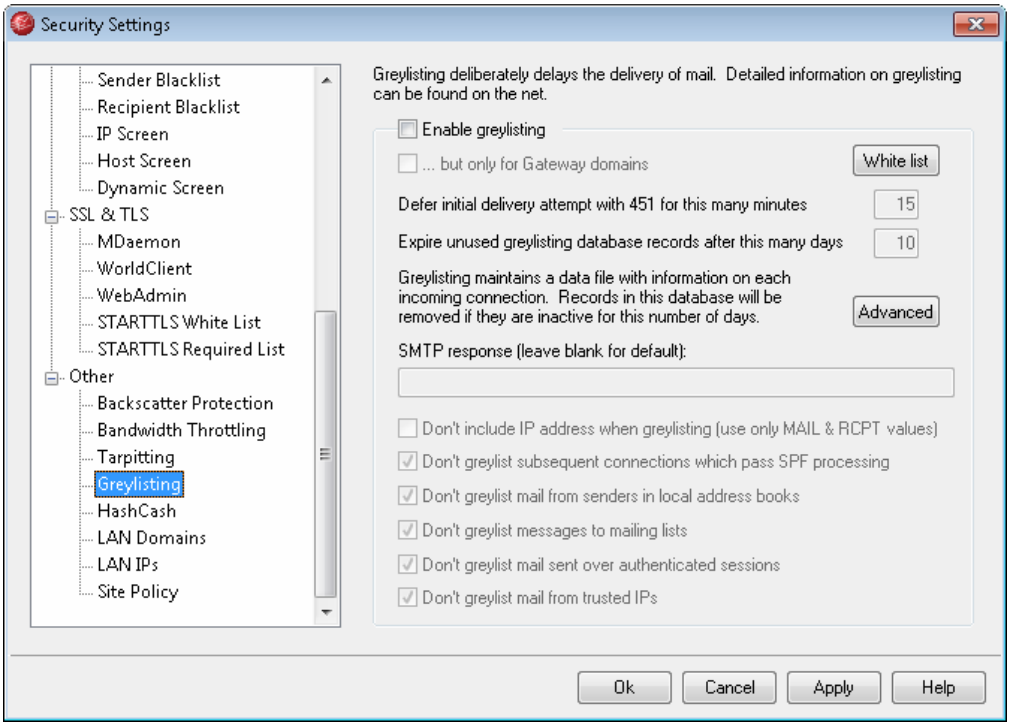
**Scaling factor**
This value is a multiplier by which the base tarpit delay will be increased over time. When the tarpit threshold is reached and the tarpit delay is applied to a session, each delay will be multiplied by this value to determine to length of the next delay in the session. For example, if the tarpit delay is set to 10 and the scaling factor is set to 1.5 then the first delay will be 10 seconds, the second will be 15 seconds, the third 22.5, then 33.75, and so on (i.e. 10 x 1.5 = 15, 15 x 1.5 = 22.5, etc.). The default Scaling factor is 1, meaning that the delay will not be increased.

**Authenticated sessions are exempt from tarpitting**
Click this checkbox if you want senders who authenticate their mail session to be exempt from Tarpitting.

**White list**
Click this button to open the Tarpitting white list. On it you can designate IP addresses that you wish to be exempt from tarpitting.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.5.4 Greylisting




Greylisting is located under the Security dialog at: Security » Security Settings » Other » Greylisting. Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a non-white listed or otherwise previously unknown sender, its sender, recipient, and sending server 's IP address will be logged and then the message will be refused by Greylisting during the SMTP session with a temporary error code. Furthermore, for a designated period of time (say, 15 minutes) any future delivery attempts will also be temporarily refused. Because "spammers" do not typically make further delivery attempts when a message is refused, greylisting can significantly help to reduce the amount of spam your users receive. But, even if the spammers should attempt to retry delivery at a later time, it is possible that by that time the spammers will have been identified and other spam-fighting options (such as DNS Black Lists 264) will successfully block them. It's important to note, however, that this technique can deliberately delay "good" email along with the "bad". But, the legitimate messages should still be delivered sometime later after the greylisting period has expired. It is also important to note that you have no way of knowing how long the sending servers will wait before making further delivery attempts. It is possible that purposely refusing a message with a temporary error code could cause it to be delayed by as little as just a few minutes or by as much as an entire day.

There are several traditional problems and negative side-effects associated with greylisting, and the Greylisting screen contains a number of options designed to deal with them.

First, some sending domains use a pool of mail servers to send outbound mail. Since a different mail server could be used for each delivery attempt, each attempt would be

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

treated as a new connection to the greylisting engine. This could multiply the length of time it would take to get past Greylisting because each of those attempts would be greylisted as if they were separate messages instead of retries of a previous message. By utilizing an SPF lookup option, this problem can be solved for sending domains who publish their SPF data. Furthermore, there is an option to ignore the IP of the sending mail server completely. Using this option lowers the efficiency of greylisting, but it does completely solve the server pool problem.

Second, greylisting traditionally entails a large database since each incoming connection must be tracked. MDaemon minimizes the need to track connections by placing the Greylisting feature nearly last in the SMTP processing sequence. This allows all of MDaemon's other options to refuse a message prior to reaching the greylisting stage. As a result, the size of the greylisting data file is greatly reduced, and since it is memory resident there is little practical performance impact.

Finally, several options are available to minimize the impact of greylisting on "good" messages. First, messages sent to mailing lists can be excluded. Next, Greylisting has its own white list file on which you can designate IP addresses, senders, and recipients that you wish to be exempt from greylisting. Finally, Greylisting contains an option for using each account's private address book files as a white list database. So, mail to a user from someone in that user's address book can be excluded from greylisting.

For more information about greylisting in general, visit Even Harris' site at:

http://projects.puremagic.com/greylisting/

### Greylisting

**Enable greylisting**
Click this option to enable the Greylisting feature within MDaemon.

**...but only for Gateway domains**
Click this check box if you only wish to greylist messages destined for gateway domains.

**White list**
This button opens the Greylisting white list on which you can designate senders, recipients, and IP addresses that will be exempt from greylisting.

**Defer initial delivery attempt with 451 for this many minutes**
Designate the number of minutes for which a delivery attempt will be greylisted after the initial attempt. During that period of time, any subsequent delivery attempts by the same server/sender/recipient combination (i.e. "greylisting triplet") will be refused with another temporary error code. After the greylist period has elapsed, no further greylisting delays will be implemented on that triplet unless its Greylisting database record expires.

**Expire unused greylisting database records after this many days**
After the initial greylisting period has elapsed for a given greylisting triplet, no further messages matching that triplet will be delayed by Greylisting. However, if no message matching that triplet is received for the number of days designated in this option, its Greylisting database record will expire. A subsequent attempt by that triplet will cause a new Greylisting record to be created it will have to go through

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the initial greylisting period again.

**Advanced**
Click this button to open the Greylisting database, which you can use to review or edit your greylisting triplets.

**SMTP response (leave blank for default)**
If you provide a custom string of text in this space then MDaemon will return the SMTP response, "`451 <your custom text>`" rather than the default "`451 Greylisting enabled, try again in X minutes`." This is useful, for example, if you wish to provide a string that contains a URL to a description of greylisting.

**Don't include IP address when greylisting (use only MAIL & RCPT values)**
Click this check box if do not wish to use the sending server's IP address as one of the greylisting parameters. This will solve the potential problem that can be caused by server pools, but it will reduce Greylisting's efficiency.

**Don't greylist subsequent connections which pass SPF processing**
When using this option, if an incoming message matches a triplet's sender and recipient but not the sending server, but SPF processing determines that the sending server is a valid alternate to the one listed in the triplet, then the message will be treated as a subsequent delivery matching that triplet rather than a new connection requiring a new Greylisting record.

**Don't greylist mail from senders in local address books**
Click this option if you wish to exempt a message from greylisting when its sender is listed in the recipient's address book.

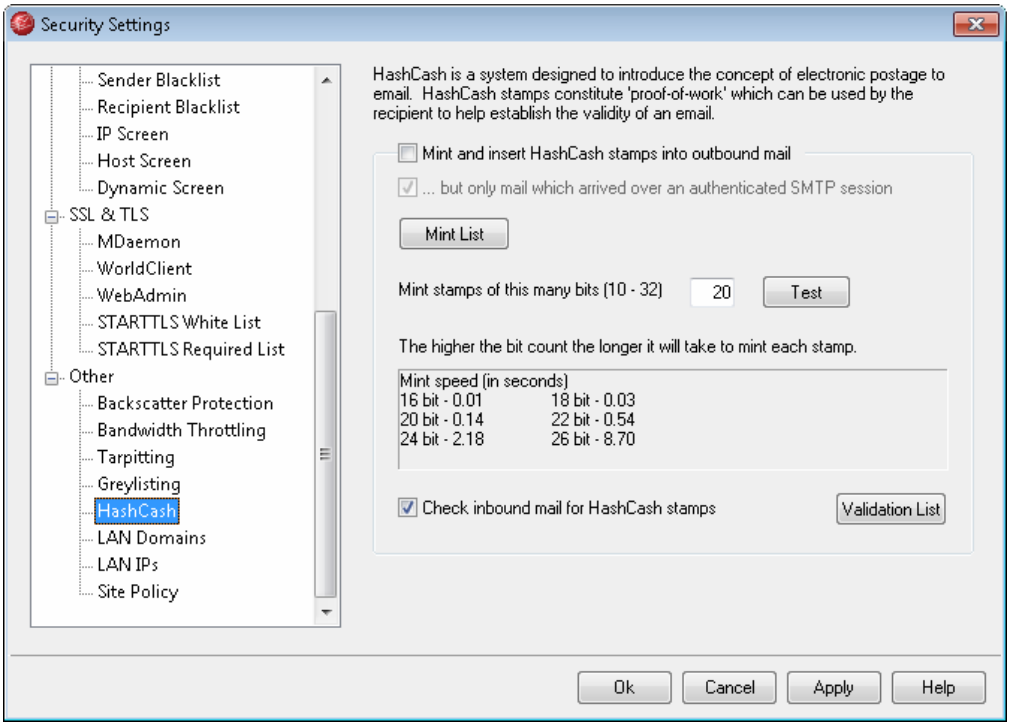
**Don't greylist messages to mailing lists**
Click this check box if you wish to exempt mailing list messages from greylisting.

**Don't greylist mail sent over authenticated sessions**
Use this option if you wish all messages coming in over an authenticated session to be exempt from greylisting.

**Don't greylist mail from trusted IPs**
Use this option if you wish all messages coming from trusted IP addresses to be exempt from greylisting.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 5.4.5.5 HashCash




HashCash is a "proof of work" system that is both an anti-spam tool and a Denial of Service countermeasure similar to an electronic form of postage. Using the HashCash system MDaemon can mint HashCash stamps, which are in effect "paid for" with CPU processing time rather than actual currency. A HashCash stamp is inserted into an outgoing message's headers and then verified by the recipient's email server and weighed according to the value of the stamp. Stamped messages are more likely to be legitimate and can therefore be passed through the receiving server's anti-spam systems. Use of HashCash stamps can help to reduce false positives and prevent messages from being erroneously rejected due to their failing to pass a word-filter or blacklist system.

Spammers rely on the ability to send many hundreds or even hundreds of thousands of messages in extremely short periods of time, and they frequently send a single copy to many recipients by using BCC and similar techniques that do not require a significant amount of processing time for any given recipient. A spammer attempting to use a HashCash system, however, would have to mint a unique HashCash stamp for each recipient each time that recipient was sent a message. This would be highly prohibitive and inefficient for the typical spammer. Conversely, for the typical legitimate mail server and sender, the extra cost in CPU time required to stamp outgoing messages is essentially insignificant and will not affect mail delivery speeds or mail processing time in any noticeable way, especially since outgoing mailing list messages are never stamped.

Stamps are only generated for outbound remote messages that are either from or to the addresses designated on the Mint List, and they are never generated for mailing list messages. Further, by default MDaemon will only generate those HashCash stamps when the message arrives via an authenticated SMTP session. Requiring authenticated sessions is recommended but optional. You can deactivate this requirement if you wish

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

to stamp messages arriving on unauthenticated sessions.

For incoming messages, only stamps contained in messages for recipients designated on the Validation List will be checked for validity. If an incoming message contains a HashCash stamp but the recipient isn't on the list, then the stamp will be ignored and the message will be processed normally as if it didn't contain a HashCash stamp at all. By default, only your Default Domain is contained on this list. Click the *Validation List* button if you wish to add other domains or domain gateways to it.

For more information on HashCash, visit http://www.hashcash.org/.

### HashCash

**Mint and insert HashCash stamps into outbound mail**
Click this check box to activate the HashCash system. MDaemon will generate stamps for outbound remote messages that are either from or to the addresses designated on the Mint List

**...but only if message arrived via AUTH'ed SMTP session**
Click this check box if you wish to generate stamps only for those messages arriving on authenticated SMTP sessions. Clear it if you do not wish to require authentication, but this is not recommended.

**Mint List**
Click this button to open the Mint List. MDaemon will only generate HashCash stamps for addresses on this list. By default only your Default Domain is listed. If you wish to generate stamps for your other domains, domain gateways, or for messages addressed either to or from specific individuals then you will need to add those addresses to the list.

**Mint stamps of this many bits (10-32)**
This is the bit count MDaemon will use when generating HashCash stamps. The larger the count the greater the amount of processing time required to generate a stamp.

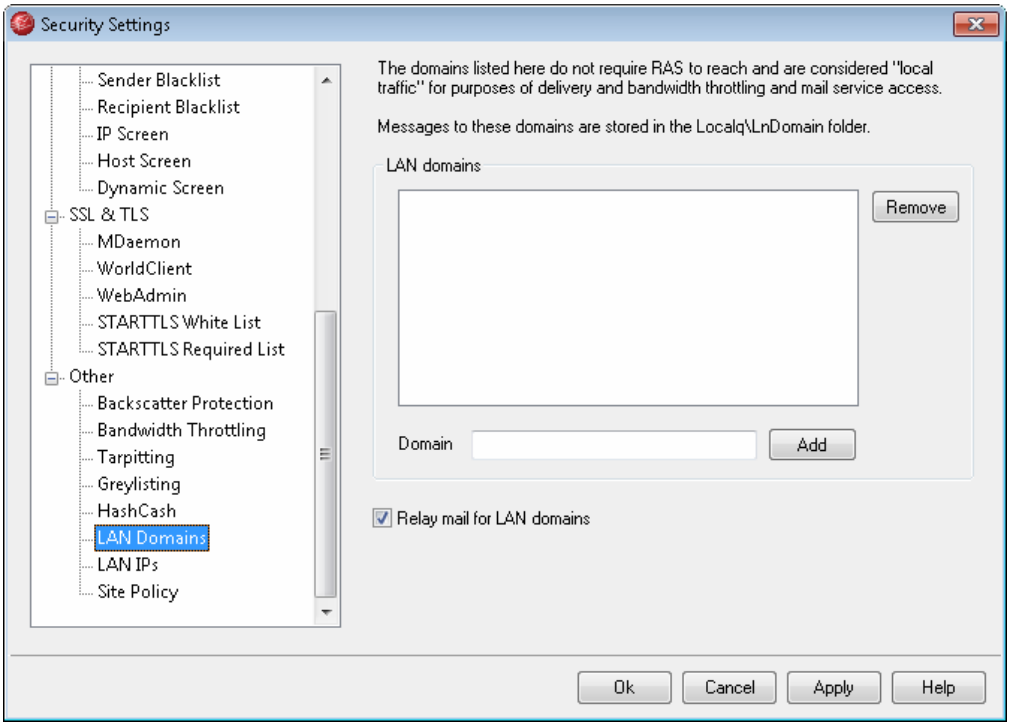
**Test**
Click this button to test the amount of time required to generate a stamp with the designated bit count.

**Check inbound mail for HashCash stamps**
Enable this option if you wish to check inbound messages for HashCash stamps and adjust their spam scores based on the results. Only messages with recipients specified on the Validation List will be checked. If an incoming message contains a HashCash stamp but the recipient isn't on the list, then the stamp will be ignored and the message will be processed normally as if it didn't contain a HashCash stamp at all.

**Validation List**
MDaemon will only attempt to validate HashCash stamps in messages for recipients designated on the Validation List. Incoming messages for recipients who are not on the list will be processed normally. No HashCash stamp check will be performed. Only your Default Domain is listed by default.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 5.4.5.6 LAN Domains




**LAN Domains**

The domains listed here are considered by MDaemon to be part of your local LAN (local area network). Therefore, no dialup or Internet connection is required in order to deliver a message to one of them.

**Domain**
Enter a domain name and then click *Add* to add it to the list.

**Add**
After specifying a domain in the *Domain* option above, click this button to add it to the list.

**Remove**
Select a domain in the list and then click this button to remove it.

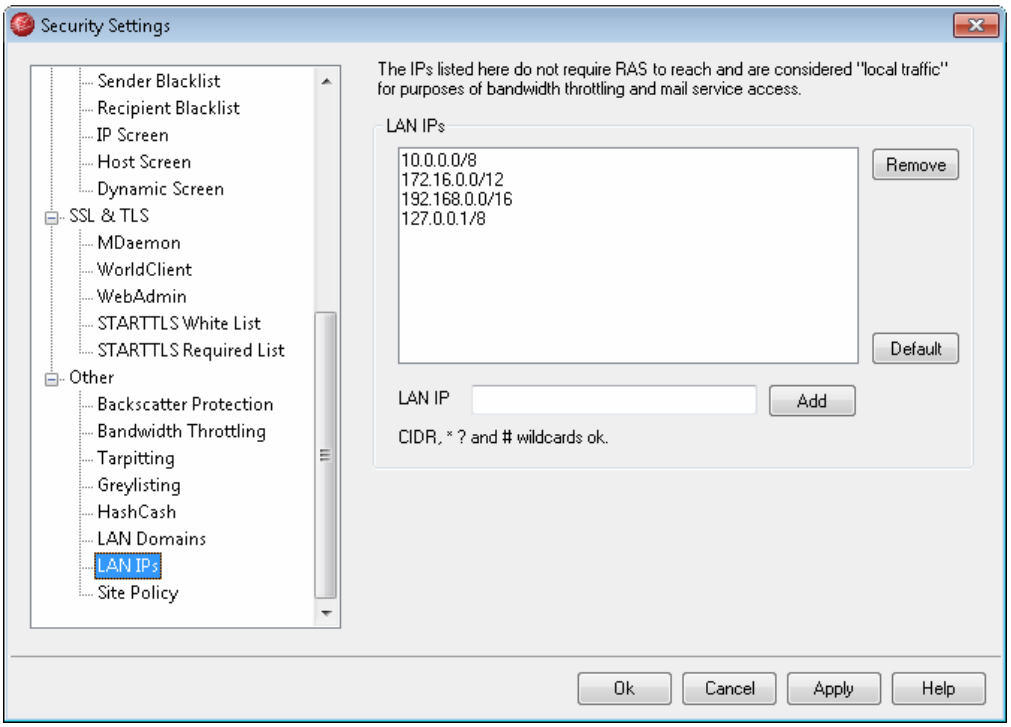
**Relay mail for LAN domains**
If this box is checked MDaemon will relay mail for these domains. This provides some measure of control over the traffic sent to and from these domains.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**See:**

LAN IPs 336

### 5.4.5.7 LAN IPs




**LAN IPs**

Similar to LAN Domains 335, this screen is used to list IP addresses that reside on your LAN (local area network). These IP addresses therefore do not require RAS or an Internet connection to reach them, and they are treated as local traffic for the purposes of bandwidth throttling. Further, there are various other security and spam prevention restrictions that they may be exempt from since they are local addresses.

**Remove**
Select an IP address from the list and then click this button to remove it.

**LAN IP**
Enter an IP address to add to the LAN IPs list and click *Add*. Wildcards like 127.0.*.* are permitted.

**Add**
After entering an IP Address into the *LAN IP* control, click this button to add it to the list.

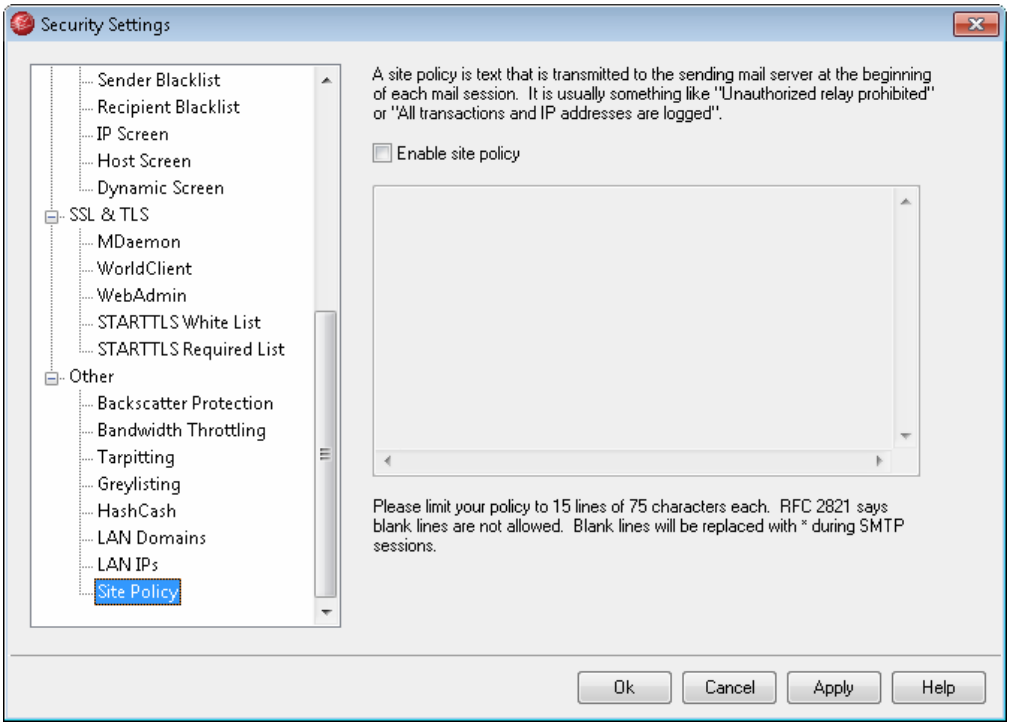
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Default**
Click this button to replace the current list of LAN IP entries with the default values that cover reserved IP address ranges. You will be asked to confirm your decision before the list is reset.

**See:**

**LAN Domains** 335

### 5.4.5.8 Site Policy




**Creating an SMTP Site Policy Statement**
Use this dialog to specify a Site Policy statement for your server. The text is stored in the `policy.dat` file located in MDaemon's `\app\` subfolder and is transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "`This server does not relay`" or "`Unauthorized use prohibited.`" You do not need to prepend each line with "`220`" or "`220-`". MDaemon handles each line accordingly, either with or without these prepended codes.

A site usage policy with a statement regarding relaying of mail would look like this during the SMTP transaction:

```
220-Alt-N Technologies ESMTP MDaemon
220-This site does relay unauthorized email.
220-If you are not an authorized user of our server
220-then you must not relay mail through this site.
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

```
220
HELO example.com...
```

The POLICY.DAT file must be comprised of printable ASCII text only and have no more than 512 characters per line; however it is highly recommended that you use no more than 75 characters per line. The maximum size of this file is 5000 bytes. MDaemon will not display files larger than 5000 bytes.

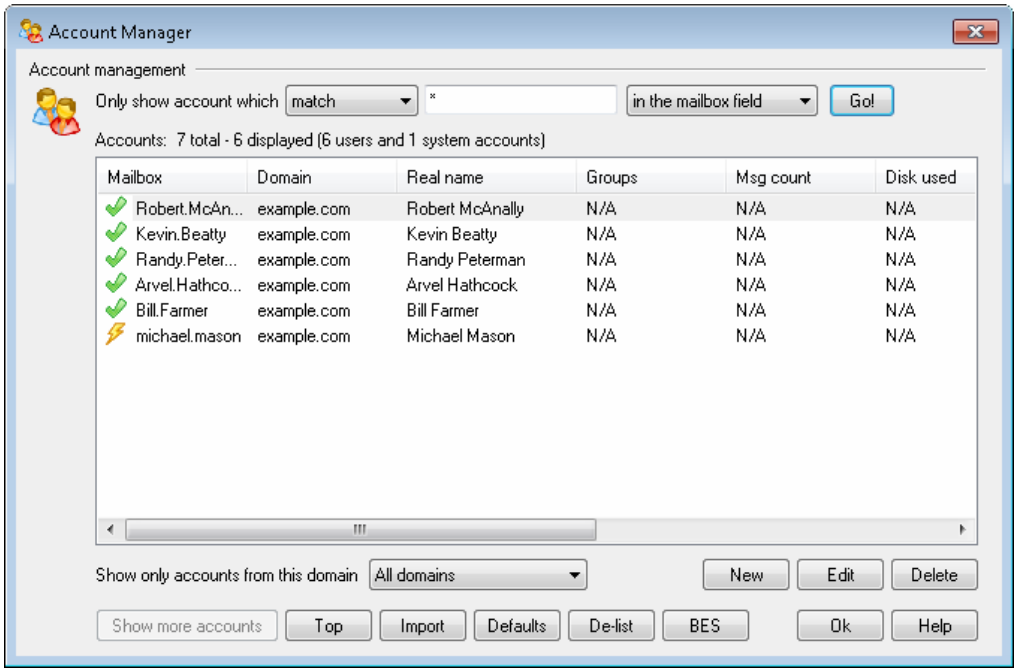
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# Section VI

# 6 Accounts Menu

## 6.1 Account Manager

To better manage the selection, addition, deletion, or modification of your accounts, MDaemon contains the Account Manager. This dialog provides access to account information and can be used to sort accounts by mailbox, domain, real name, or mail folder. The Account Manager is located under the Accounts menu at: Accounts » Account Manager...




### Account Management

Above the list of accounts you will see two statistics regarding the list. The first number is the total number of MDaemon user accounts that currently exist on your system. The second number is the number of those accounts currently displayed in the list. The accounts that will be displayed is contingent upon what you have chosen in the *Show only accounts from this domain* option below the list. If you have selected "All Domains" then all of your MDaemon accounts will be displayed in the list. There is a search option at the top of this dialog that you can use to define exactly which accounts will be displayed beyond simply the domain to which they belong.

Each entry in the list contains an Account Status Icon (see below), the mailbox, the domain to which it belongs, the "real name" of the account holder, any groups to which the account belongs, the message count, the disk space used (in MB), and the mail folder in which the account's messages are stored. This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

By default, only 500 accounts at a time will be displayed in this list. If you want to see more accounts from the currently selected domain (or All Domains, if you have selected that option) then you must click the *Show more accounts* button to display the next 500. If you want to be able to display more than 500 accounts at a time then open the `MDaemon.ini` file and change the `MaxAccountManagerEntries=500` key to whatever value that you prefer.

### Account Status Icons

Account is a global or domain administrator.

Full access account. Both POP and IMAP access are enabled.

Restricted access account. Either POP or IMAP access is disabled.

Restricted access account. Both POP and IMAP access are disabled.

Disabled account. All access to the account is disabled.

**Show only accounts from this domain**
Choose "All Domains" from this drop-down list box to display all MDaemon accounts. Choose a specific domain to show only that domain's accounts.

**New**
Click this button to open the Account Editor 343 in order to create a new account.

**Edit**
Select an account from the list and then click this button to open it in the Account Editor 343.

**Delete**
Select an account from the list and then click this button to delete it. You will be asked to confirm your decision to delete the account before MDaemon will proceed.

**Show more accounts**
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500. See the note above for instructions on how to increase the maximum number of accounts that may be displayed.

**Top**
Click this button to quickly move to the top of the account list.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Import**
Click this button if you wish to import accounts from a comma delimited text file. This button is identical to the Accounts » Importing » Import accounts from a comma delimited text file menu selection.

**Defaults**
Click this button to open the New Account Defaults 380 dialog.

**De-list**
Select one or more accounts and then click this button if you wish to unsubscribe them from all Mailing Lists 433 hosted on the server. A box will open asking you to confirm the decision to remove the addresses from the lists.

**BES**
Select one or more accounts and then click this button to enable them for BlackBerry device synchronization 351. You will be asked to confirm your decision to enable the accounts. This has the same effect as separately opening each account's BlackBerry Enterprise Server screen and clicking the *Enable BlackBerry device synchronization* option.

---

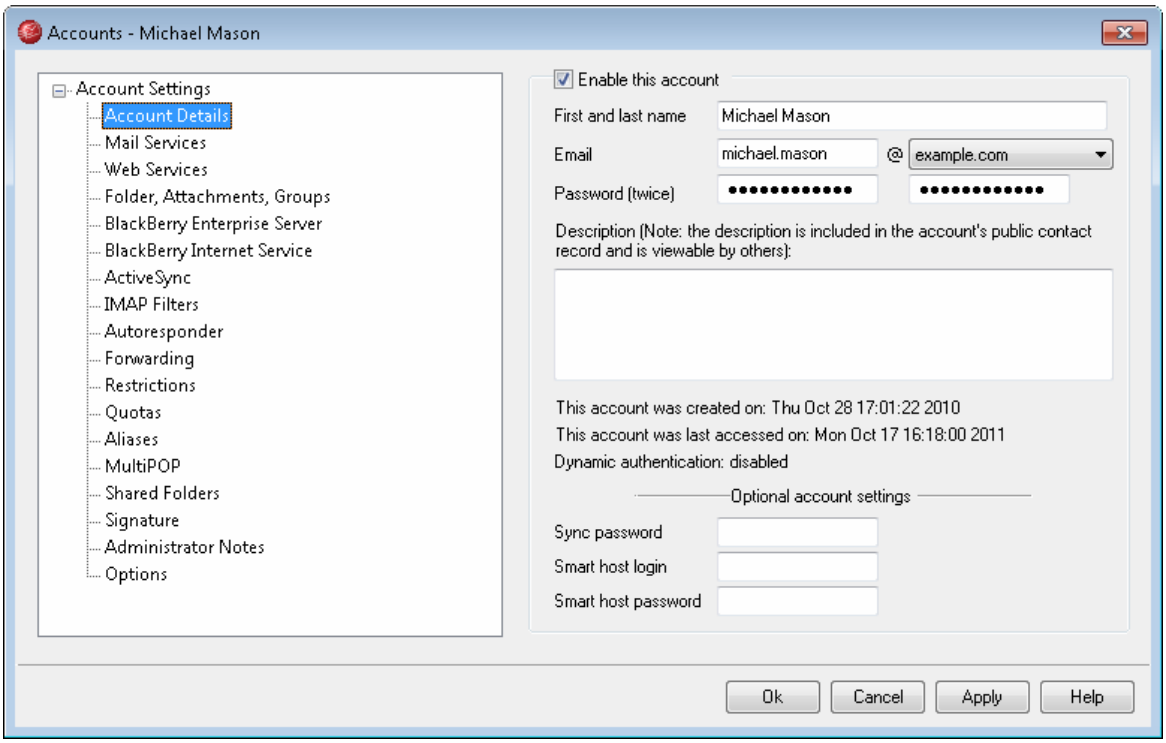
**See:**

**New Account Defaults** 380
**Account Editor** 343

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 6.1.1 Account Editor

### 6.1.1.1 Account Details




**Account Settings**

**Enable this account**
Clear this checkbox if you wish to disable all access to the account. The user will not be able to access the account by any means, nor will MDaemon accept mail for it. It will not be deleted, and it will still count toward the number of accounts used in your license's account limit, but MDaemon will operate as if the account doesn't exist.

**First and last name**
Enter the user's first and last name here. When creating a new account, most of the fields on the various screens of the Account Editor will be automatically filled in while typing the first and last name of the user. This auto-generated information is based on the templates and settings found in New Account Defaults 380. The first and last name field cannot contain " ! " or " | ".

**Email address**
Use this field to specify the email address for the account. When creating a new account, the mailbox portion of the address will be filled in for you automatically while you type the *First and last name* above, based on the *Mailbox template* designated under: New Account Default » Mailbox 380. You can manually enter a different mailbox name if you do not wish to use the one that is generated for you. Next, click the drop-down list box after the "@" symbol to pick the domain to which the account will belong. MDaemon's Default Domain 41 will appear in the drop-down

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

list by default. The complete email address is used as the unique identifier for the account and as its login for POP3, IMAP, WorldClient, and so on. Email addresses cannot contain spaces or " ! " or "|" characters.

**Password (twice)**
This is the password that the account will use when connecting to MDaemon to send or receive email via POP3 or IMAP, when authenticating during the SMTP process, or when using WorldClient, WebAdmin, or Outlook Connector. Below this area is a short statement identifying whether or not Dynamic Authentication 425 is being used for the account.

You should always provide an *Email password* even if you do not wish to allow POP3/IMAP access to the mail account. In addition to mail session verification, *Email address* and *Email password* values are used to allow remote account configuration and remote file retrieval. If you wish to prevent POP/IMAP access, use the options located on the Mail Services 345 screen. If you wish to prevent all access, then uncheck the *Enable this account* option.

**Description**
Use this text area if you wish to add a public description of the account.

This description is included in the account's public contact record and is viewable by others. Do not include private or sensitive information in this field. For private notes or comments regarding this account, use the Administrator Notes screen.

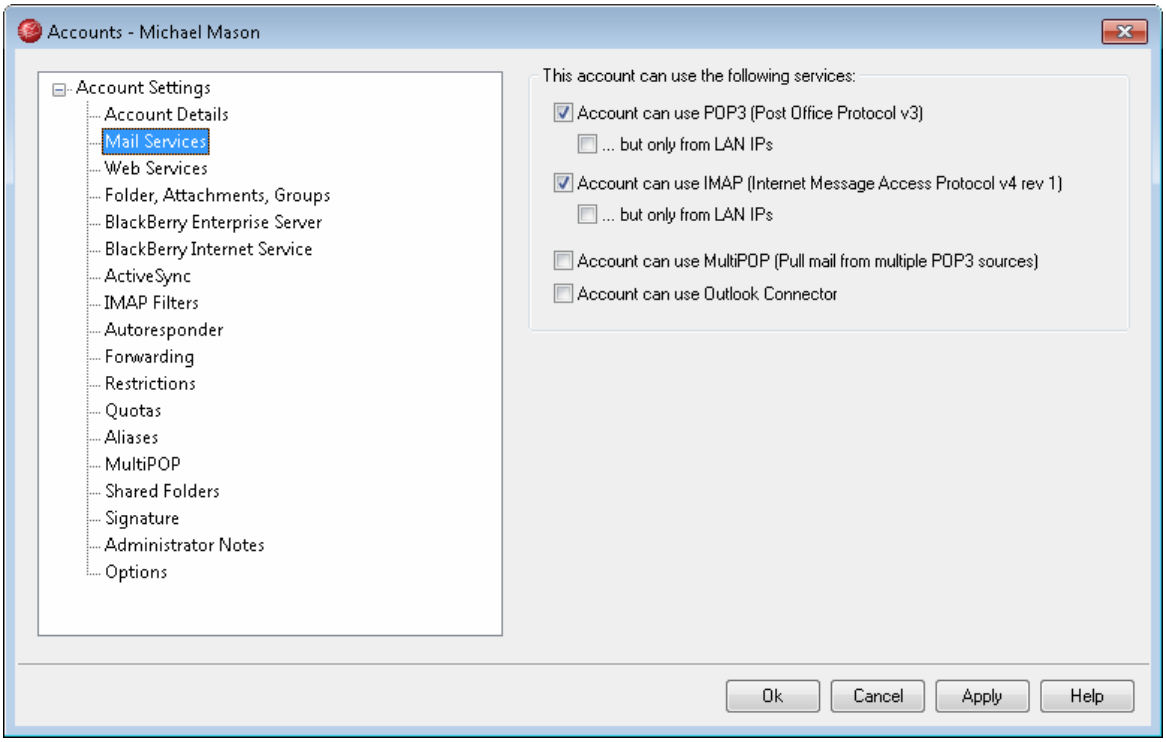
## Optional Account Settings

**Sync password**
Use this option if you wish to designate a different password for the account to use when interacting with a synchronization server, such as SyncML 191 or ActiveSync 154. If no sync password is assigned then the account's *Email password* is used for sync connections. For accounts using Dynamic Authentication, however, a sync password is necessary—they cannot log in to the Sync server via Dynamic Authentication.

**Smart host login/password**
If the *Allow per-account authentication* option is enabled on the Delivery 43 screen at Setup » Default Domain/Servers, and you wish to use per-account authentication with this account instead of using the credentials specified on that screen, then specify the account's optional smart host credentials here. If you do not wish to use per-account authentication for this account then leave this option blank.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.1.1.2 Mail Services




The options on this screen govern which mail services the account is allowed to use: POP3, IMAP, MultiPOP, Outlook Connector. Email access via WorldClient is controlled from the Web Services 346 screen.

**This account can use the following services:**

**Account can use POP3 (Post Office Protocol v3)**
When this box is checked, the account's mail can be accessed via Post Office Protocol v3 (POP3). Virtually all email client software supports this protocol.

**...but only from LAN IPs**
Check this box if you wish to allow the account to be accessed via POP3 only when the user is connecting from a LAN IP address 336.

**Account can use IMAP (Internet Message Access Protocol v4 rev 1)**
When this box is checked, the account's mail can be accessed via Internet Message Access Protocol v4 rev 1 (IMAP4). IMAP is more versatile than POP3, allowing email to be managed on the server and accessed using multiple clients. Most email client software supports this protocol.

**...but only from LAN IPs**
Check this box if you wish to allow the account to be accessed via IMAP only

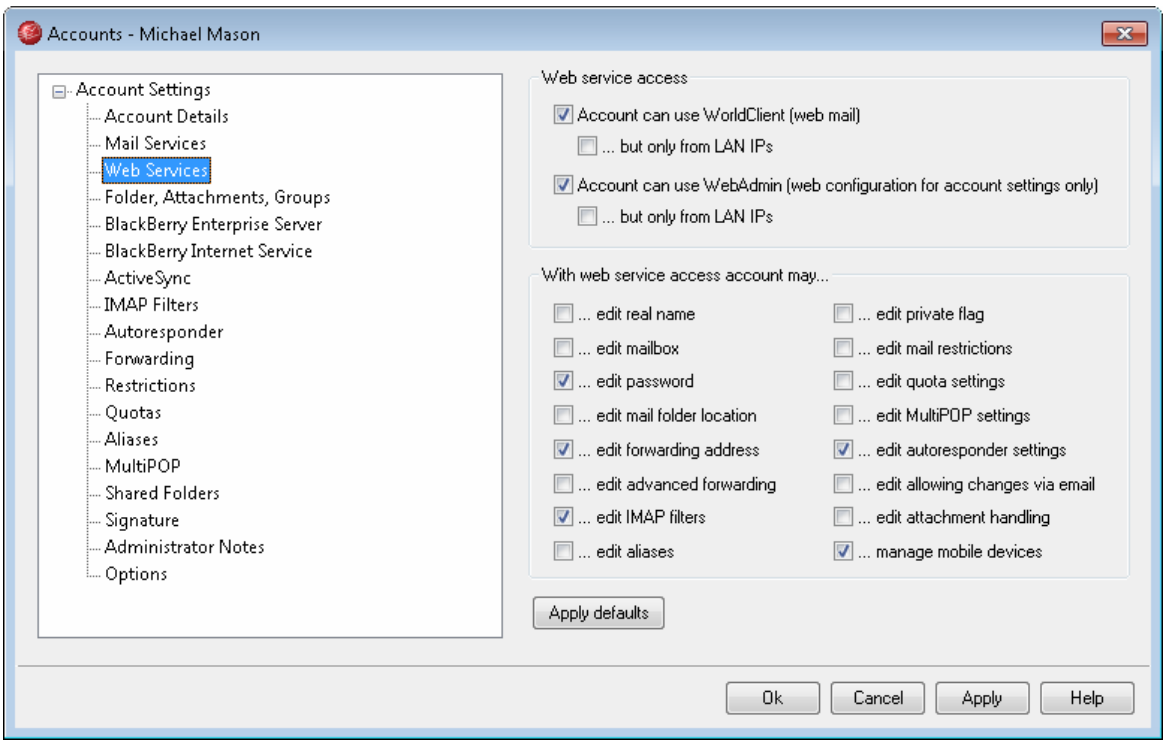
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

when the user is connecting from a LAN IP address[336].

**Account can use MultiPOP (Pull mail from multiple POP3 sources)**
Check this box if you wish to allow the account to use MultiPOP[369]. MultiPOP allows the user to collect mail from other email accounts, maintained on other mail servers.

**Account can use Outlook Connector v2.x**
Click this option if you wish to allow the account to share Microsoft Outlook folders using Outlook Connector for MDaemon[408]. **Note:** this option will only be available when Outlook Connector is installed.

### 6.1.1.3 Web Services




#### Web Service Access

**Account can use WorldClient (web mail)**
Enable this checkbox if you want the account to be able to access the WorldClient[111] server, which enables users to check their email using a web browser.

**...but only from LAN IPs**
Check this box if you wish to allow the account access to WorldClient only when connecting from a LAN IP address[336].

**Account can use WebAdmin (web configuration for account settings only)**
Check this box if you wish to grant the user permission to modify his or her account settings via WebAdmin[132]. The user will only be able to edit those settings that you enable below.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

When this feature is enabled and the WebAdmin server is active, the user will be able to log in to WebAdmin by pointing a browser to the designated MDaemon domain and port assigned to WebAdmin 134 (e.g. `http://example.com:1000`). He will first be presented with a sign-in screen and then a screen that contains the settings that he has been given permission to edit. All he needs to do is edit whatever settings he chooses and then click the *Save changes* button. He can then sign out and close the browser. If he has access to WorldClient then he can also access WebAdmin from the Advanced Options menu within WorldClient.

If the user is a Global or Domain Administrator (designated on the Account Editor's Options 377 screen) he will see a different screen after he logs in to WebAdmin.

**...but only from LAN IPs**
Check this box if you wish to allow the account access to WebAdmin only when connecting from a LAN IP address 336.

### With web service access account may...

**...edit real name**
Enabling this feature will allow the user to modify the account's *First and last name* setting.

**...edit mailbox**
Enabling this feature will allow the user to modify the mailbox portion of his or her *Email address*.

Because the mailbox is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

**...edit password**
Click this checkbox if you wish to allow the user to modify the account's *Email password.*

**...edit mail folder location**
Checking this box gives the user permission to modify the account's Message Folder 349.

You should exercise caution in granting this permission to users. Giving users permission to change their message folder effectively gives them the ability to affect any folder on your server.

**...edit forwarding address**
When this feature is enabled, the user will be able to modify the forwarding 362 address settings.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...edit advanced forwarding**
When this feature is enabled, the user will be able to modify the *Advanced Forwarding Options*.

**...edit IMAP filters**
Use this control to enable the user to create and manage his own mail filters[356]. This feature is only available in MDaemon PRO.

**...edit aliases**
Enable this option if you wish to allow the accountholder to use WebAdmin to edit Address Aliases[368] associated with his or her account.

**...edit private flag**
This option governs whether or not the user will be permitted to use WebAdmin to edit the "*Account is private*" option located on the Account Editor's Options[377] screen.

**...edit mail restrictions**
This checkbox controls whether or not the account will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions[364] screen.

**...edit quota settings**
Click this checkbox if you wish to allow the account to modify the quota[366] settings.

**...edit MultiPOP settings**
Click this checkbox if you wish to give the account permission to add new MultiPOP[369] entries and to enable/disable MultiPOP collection for those entries.

**...edit autoresponder settings**
Click this checkbox if you wish to give the user permission to add, edit, or delete Autoresponders[359] for his account.

**...edit allow changes via email**
Click this checkbox if you wish to allow the user to modify his *Account Settings* via specially formatted email messages[504].

**...edit attachment handling**
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Folder, Attachments, Groups[349] screen.

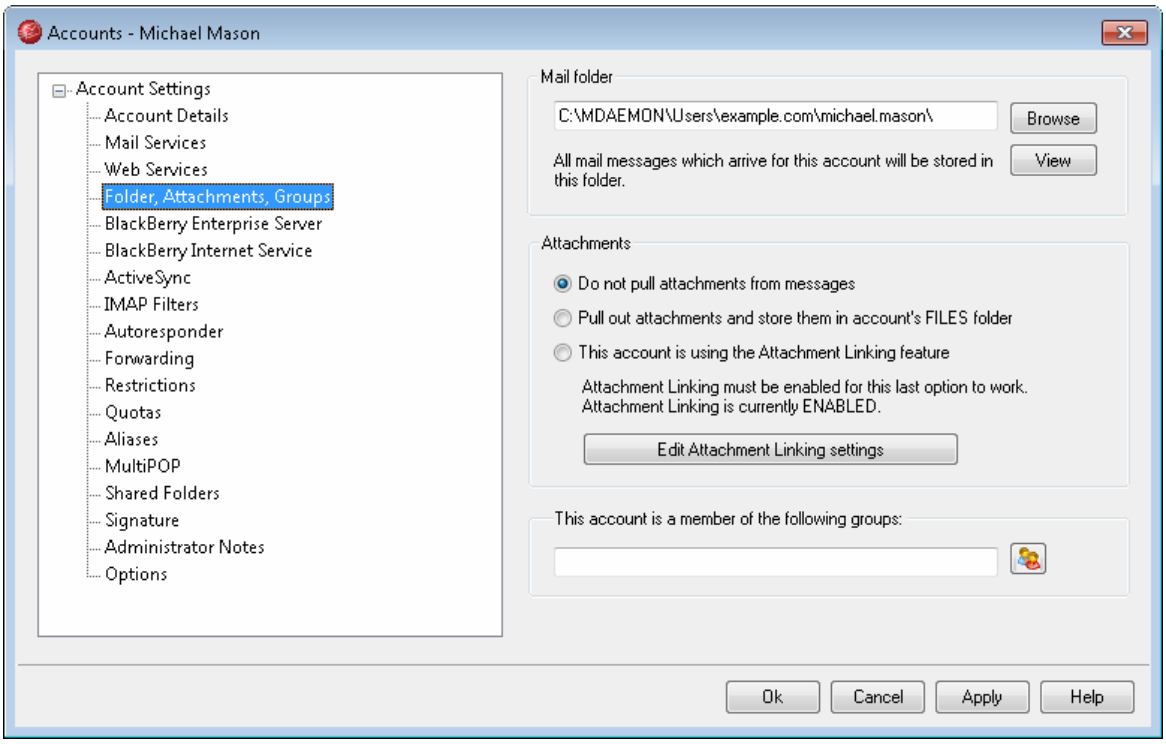
**...manage BlackBerry device**
Use this option if you wish to allow the accountholder to use WebAdmin to manage his or her BlackBerry Enterprise Server[351] settings.

**Apply defaults**
Click this button to return the settings on this screen to the default values designated on the Web Services[387] screen located at: Accounts » Account Settings

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

» New Account Defaults.

### 6.1.1.4 Folder, Attachments, Groups




#### Mail Folder

Enter the folder where you wish to store this account's email messages. When creating a new account, the default location of this folder is based on the *Mail folder template* designated under: New Account Default » Mailbox 380.

#### Attachments

**Do not pull attachments from messages**
If this option is selected, attachments will not be extracted from the account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

**Pull out attachments and store them in the account's FILES folder**
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages for this account. Extracted files are removed from the incoming message, decoded, and placed in the account's `\Files\` subfolder. A note is then placed within the body of the message, stating the names of the files that were extracted. This option does not provide a link to the stored attachments, therefore the user would need the appropriate network access rights to retrieve them.

**This account is using the Attachment Linking feature**
This option causes attachments to be extracted from the account's incoming

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

messages and stored in the location designated on the Attachment Linking 142 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file.

If this option is selected but the Attachment Linking feature is disabled on the Attachment Linking 142 dialog, then attachments will not be extracted.

**Edit Attachment Linking settings**
Click this button to open the Attachment Linking 142 dialog.

### Groups

**This account is a member of the following groups:**
Use this box to add the account to one or more account Groups 420. Separate each group with a space, or use the Account icon to browse a list of available Groups.

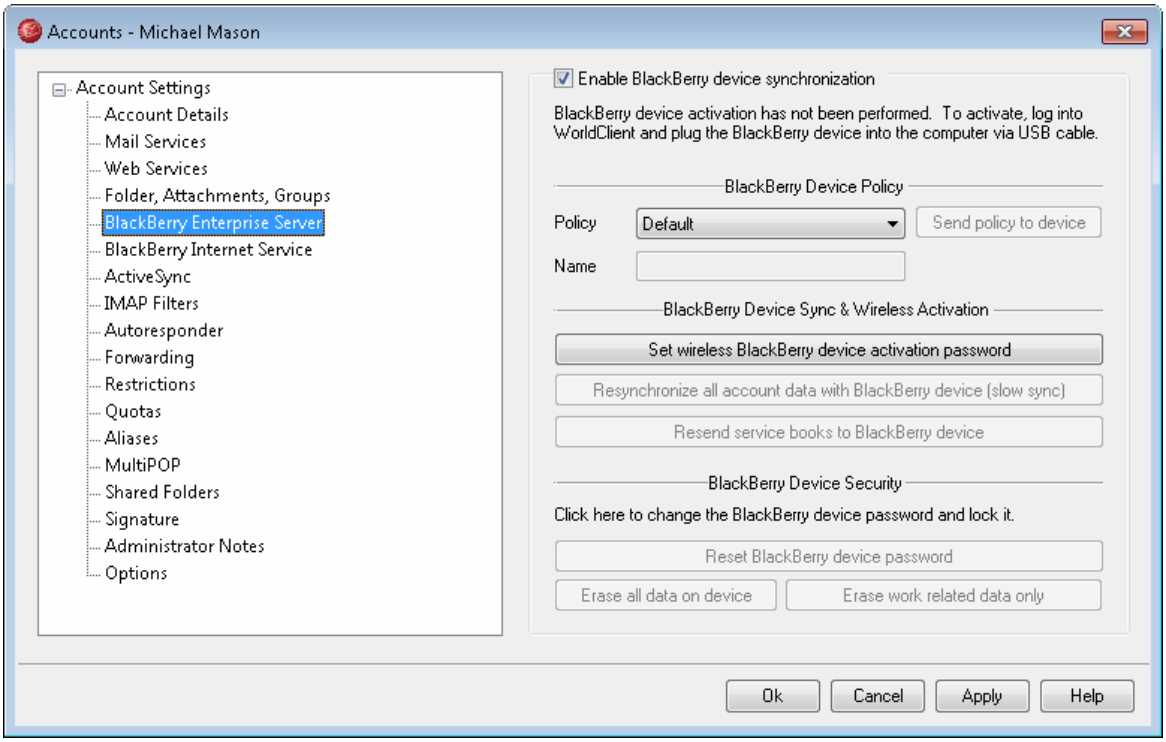
---

**See:**

**Attachment Linking** 349
**New Account Default » Mailbox** 380
**Groups** 420

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.1.1.5 BlackBerry Enterprise Server




The options on this screen govern BlackBerry Enterprise Server settings for the specific account and allow you to perform several actions regarding the account's activated BlackBerry device.

BlackBerry Enterprise Server is not available in some countries and regions.

#### Enable BlackBerry device synchronization

Click this checkbox to enable the account for BlackBerry device synchronization. BlackBerry enabled accounts appear on the BlackBerry Enterprise Server » Integrated Accounts 176 screen and can activate a BlackBerry device via USB cable in WorldClient or over the air (OTA) from the device itself (not all devices support OTA activation).

After a device is activated, its PIN, Platform version, Phone model, and Number will be listed in this section.

After an account is enabled for BlackBerry device synchronization, the BlackBerry Enterprise Server database will begin storing information about the account's messages and data so that it can be synchronized 180 with a BlackBerry device when the device is activated. All messages that have been processed for the account since being BlackBerry enabled will be synchronized with the device when it is

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

activated.

If you disable this option then all BlackBerry Enterprise Server data related to the account will be deleted. If you BlackBerry enable the account again then it will start storing data again, and the device will have to be reactivated.

### BlackBerry Device Policy

**Policy**
Choose the policy[167] from the drop-down list that you want the device to use when it is activated.

**Name**
This is the name of the account as it will appear on the activated device (for example, "Desktop," "MDaemon," "Company" or the like).

**Send policy to device**
If the device is already activated and you wish to send a new policy to it, select the policy from the drop-down list and click this button.

### BlackBerry Device Sync & Wireless Activation

**Set wireless BlackBerry Device Activation password**
To set a wireless BlackBerry Device Activation password for the account, click this button, enter a password, and click **OK**. The user can then enter the account's email address and BlackBerry Device Activation password on the device's Enterprise Activation screen to activate it OTA. Not all devices can be activated wirelessly.

**Resynchronize all account data with BlackBerry device (slow sync)**
Click this button and then click **OK** on the confirmation dialog if you wish to resynchronize all account data with the device. This is commonly called "slow sync" and ensures that the data on the BlackBerry device matches what is in MDaemon. Depending on the amount of data, this can take several minutes to complete. When slow sync starts it will run in the background until finished. There is an option located on the BlackBerry Enterprise Server » Integrated Accounts[176] screen that can be used to resynchronize **all** activated BlackBerry devices. See BlackBerry Enterprise Server » Options[179] for more BlackBerry Enterprise Server synchronization options.

**Resend service books to BlackBerry device**
If you need to resend the service books to the account's BlackBerry device, click this button and then click **Yes** on the confirmation dialog.

### BlackBerry Device Security

**Reset BlackBerry device password**
If you wish to remotely reset the device's password, click this button, enter a password, and click **OK**.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

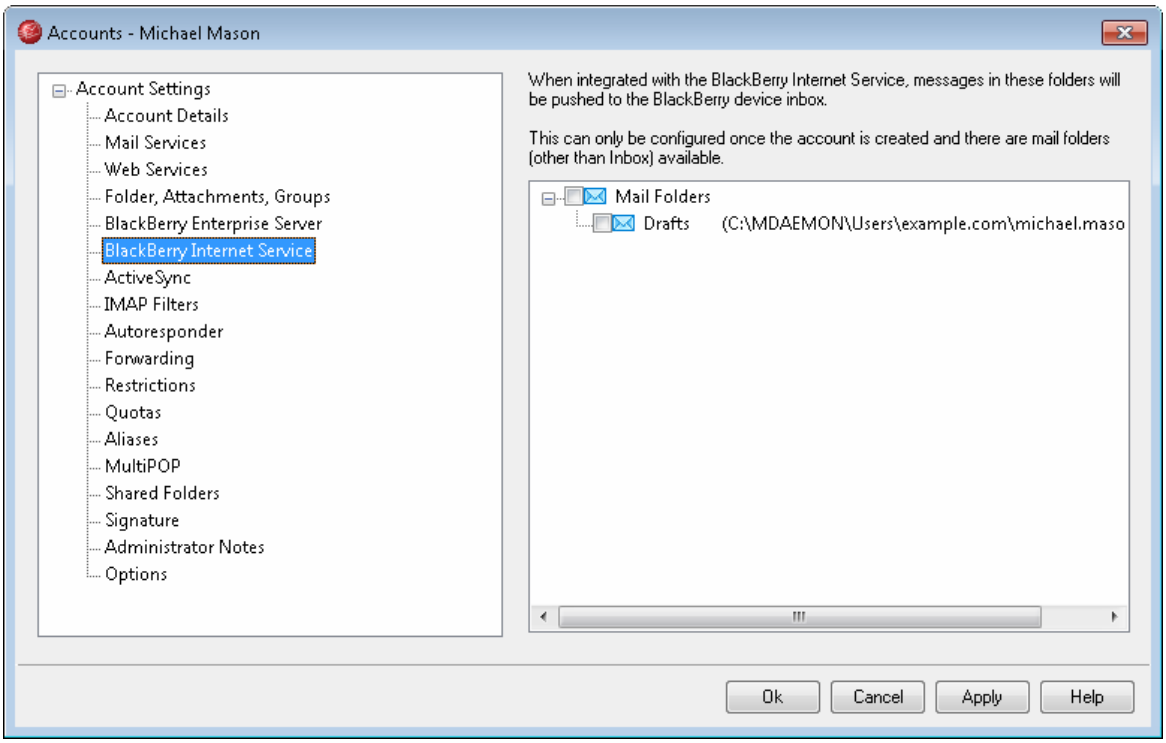
**Erase all data on device**
If you need to erase all data on the BlackBerry device remotely, such as when the device is lost or stolen, click this button and click **Yes** on the confirmation dialog.

**Erase work related data only**
Click this button if you wish to erase only work related data from the BlackBerry device, such as when it is lost or stolen. This is only supported on BlackBerry devices running OS 6.0 MR2 or higher. The BlackBerry Enterprise Server's work related data options are located under the BlackBerry Balance section of the Policies 167 screen. For more information, see: Deleting only work data from a device at blackberry.com.

**See:**

**BlackBerry Enterprise Server** 162

### 6.1.1.6 BlackBerry Internet Service




If a BlackBerry smartphone is using the BlackBerry Internet Service (BIS) to collect this account's email, you can use this screen to specify the IMAP folders whose new messages you wish to push to the smartphone's Inbox. Ordinarily the BlackBerry Internet Service only collects messages from the user's Inbox folder, not from any other folders associated with the user's account. Therefore if he or she is using IMAP filters 356 to sort messages automatically into specific folders, those messages will not

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

be delivered to the BlackBerry device. This screen makes it possible for the user to get those filtered messages from whichever folders he or she chooses. This feature does not, however, deliver messages that were already contained in any of the folders—it only delivers new messages. If the account has no IMAP filters then this screen will be blank.

The folders themselves are not pushed to the BlackBerry device, only the new messages that are placed in them. All messages will be delivered to the device's Inbox, not to any specific folders on the device.

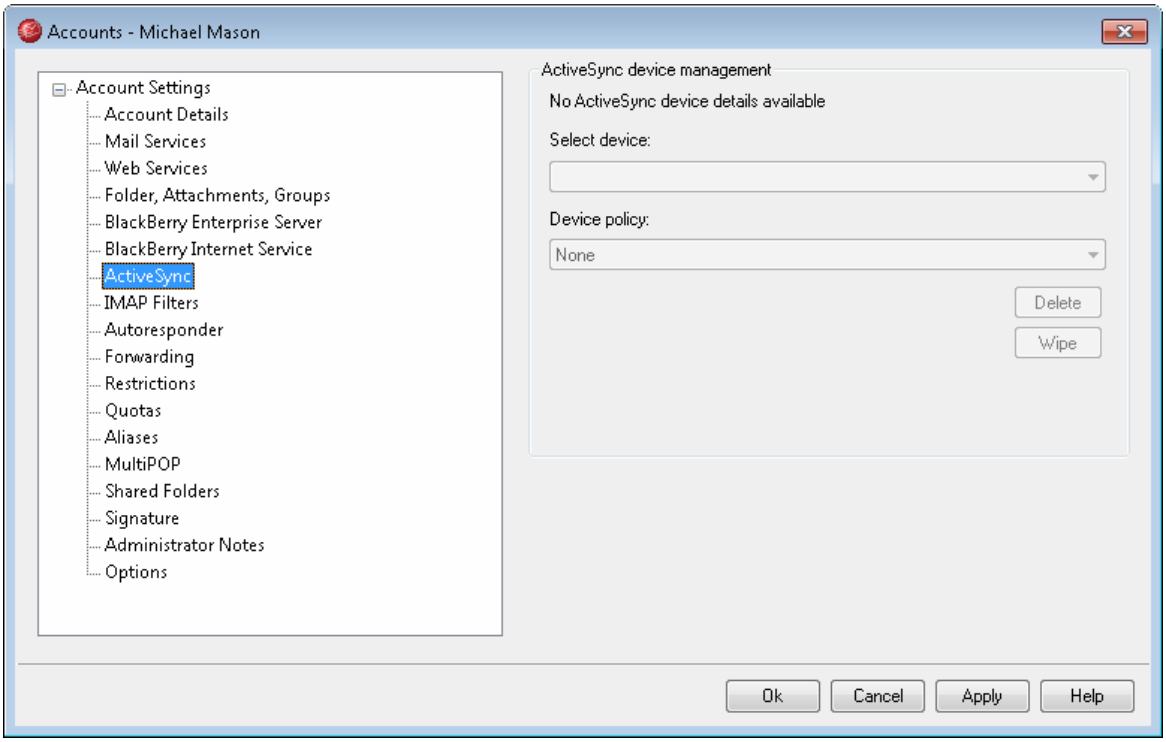
For users with access to WorldClient, the Folders page under Options in WorldClient contains this option so that users can manage the folder selection for themselves. This option, however, will only be available to them if the "*Allow selection of non-Inbox folder content to send to BlackBerry*" option on the BlackBerry Internet Service Options 189 screen is enabled.

**See:**

**BlackBerry » BlackBerry Internet Service** 183

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.1.1.7 ActiveSync




This screen displays information about any ActiveSync devices associated with the user's account. There are also options for assigning ActiveSync Policies[156] to the devices, and for deleting and remotely wiping them.

#### Assigning an ActiveSync Policy

To assign a policy to an ActiveSync device, select the device from the *Select device* drop-down list, choose a *Device policy*, and click **Ok** or **Apply**.

#### Deleting an ActiveSync Device

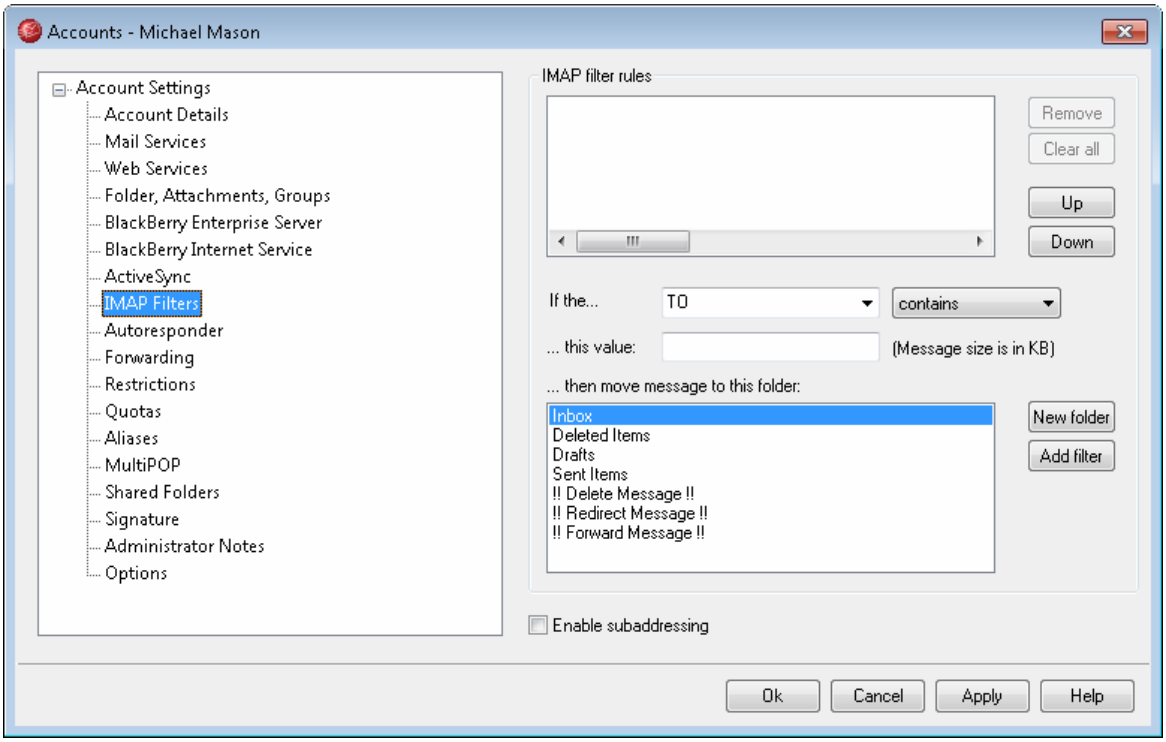
When you select an ActiveSync device from the drop-down list and click *Delete*, this will remove the device from the list and delete all synchronization data related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same device, MDaemon will treat the device as if it had never before been used on the server; all device data will have to be re-synchronized with MDaemon.

#### Remotely Wiping an ActiveSync Device

When you select an ActiveSync device from the drop-down list and click *Wipe*, the next time the device connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the device, this may remove everything on it, including downloaded apps. Further, as long as the device's ActiveSync entry exists in MDaemon, it will be wiped again if it ever connects again to MDaemon in the future. If you no longer wish to wipe the device when it connects (for example, if a lost device is recovered and you wish to use it again with the account) then you must first use the *Delete* option above to remove the device from MDaemon.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.1.1.8 IMAP Filters




With MDaemon, IMAP and WorldClient[111] users can have their mail routed automatically to specific folders on the server by using filters. Similar to the Content Filters[212], MDaemon will examine the headers of each of the account's incoming messages and then compare them to the account's filters. When a message for the account matches one of its filters, MDaemon will move it to the folder specified in that filter. This method is much more efficient (for both the client and server) than attempting to filter the messages at the client, and since some mail clients do not even support local message rules or filtering, mail filters provide this option to them.

Administrators can create filters via the IMAP Filters screen of the Account Editor, or by using WebAdmin[132]. However, you can also grant your users permission to create and manage filters for themselves from within WorldClient or WebAdmin. These permissions are set on the Web Services[346] screen.

#### IMAP filter rules

This box displays the list of all filters that have been created for the user's account. Filters are processed in the order in which they are listed until a match is found. Therefore, as soon as a message matches one of the filters it will be moved to the folder specified in that filter and then filter processing for that message will cease. Use the *Up* and *Down* buttons to move filters to different positions in the list.

#### Remove

Click a filter in the list and then click *Remove* to delete it from the list.

#### Clear all

Click this button to delete all of the user's filters.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Up**
Click a filter in the list and then click this button to move it to a higher position in the list.

**Down**
Click a filter in the list and then click this button to move it to a lower position in the list.

**If the... [message header/Size]**
Choose "*Message Size*" or a header from this drop-down list box, or type a header into the box if the desired header is not listed. When a header is designated, MDaemon will scan that header in all of the account's incoming messages for the text contained in the "*this value*" box below. Then, based upon the type of comparison being made, it will determine which messages should be moved to the filter's specified folder.

**Comparison-type**
Use this drop-down list to choose the type of comparison that will be made to the message's header or size indicated in the filter. MDaemon will scan the specified header for the text contained in the "*this value*" field (or compare the message's size to that value) and then proceed based upon this option's setting —does the message size or header's complete text match exactly, not match exactly, contain the text, not contain it at all, start with it, and so on.

**...this value**
Enter the text that you want MDaemon to search for when scanning the message header that you have specified for the filter. When the filter is set to check the message's size, set this value to the desired number of KB.

**...then move message to this folder**
After specifying the various parameters for the filter, click the folder that you want messages matching it to be moved to and then click the *Add filter* button to create the filter. This list also contains the following three special entries: "*!!Delete Message!!*," "*!!Redirect Message!!*," and "*!!Forward Message!!*."

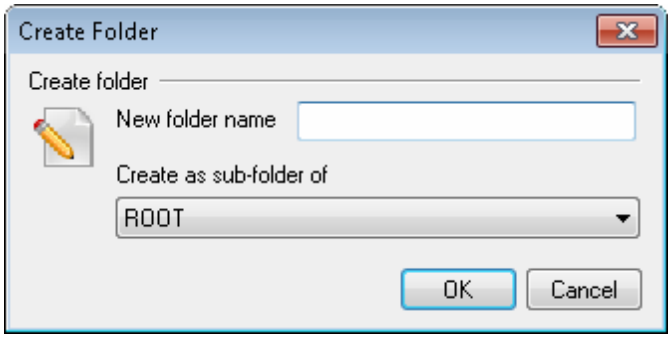
**!! Delete Message !!** – Choose your filter values, click this option in the folder list, and then click *Add filter* to create a filter that will cause a message to be deleted when it matches the filter's conditions.

**!! Redirect Message !!** – Choose your filter values, click this option in the folder list, click *Add filter*, and then enter an Email address. This will create a filter that will cause a message that meets the filter's conditions to be redirected to the designated email address. No changes to the message headers or body will be made. The only thing changed is the SMTP envelope recipient.

**!! Forward Message !!** – Choose your filter values, click this option in the folder list, click *Add filter*, and then enter an Email address. This will create a filter that will cause a message that meets the filter's conditions to be forwarded to the designated email address. A new message will be created and sent, with the Subject header and body content taken from the original message.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**New folder**
Click this button to create a new folder. This will open the Create Folder dialog on which you will assign a name for the folder. If you want it to be a subfolder of an existing folder then choose the folder from the drop-down list.




**Add filter**
When you are finished making your choices for a new filter, click this button to add it to the list.

## Subaddressing

Subaddressing is a system for including a folder name in the mailbox portion of an account's email address. Using this system, messages addressed to the *mailbox+folder* name combination will be routed automatically to the account's folder included in the address (assuming that folder actually exists), without the need to create specific filtering rules to make that happen.

For example, if `bill.farmer@example.com` has an IMAP mail folder called "`stuff`," then mail arriving addressed to "`bill.farmer+stuff@example.com`" would be routed automatically to that folder. Subfolders can be designated by including the folder and subfolder names separated by an additional "+" character, and underscores are used to replace spaces in folder names. So, using the example above, if Bill's "`stuff`" folder had a subfolder called "`my older stuff`," then messages addressed to "`bill.farmer+stuff+my_older_stuff@example.com`" would be routed automatically to Bill's "`\stuff\my older stuff\`" mail folder.

Since subaddressing requires the use of the "+" character, mailboxes that contain "+" cannot be subaddressed. So, in the example above, if the actual address were "`bill+farmer@example.com`" instead of "`bill.farmer@example.com`" then it could not be subaddressed. Further, you cannot use an address alias in a subaddress. You can, however, create an alias that refers to an entire subaddressed form. So, even though "`alias+stuff@example.com`" is not permitted, using "`alias@example.com`" to point to "`bill.farmer+stuff@example.com`" would be fine.

To prevent exploits or abuse, the IMAP folder included in the subaddress **must** be valid. If a subaddressed message arrives for an account that does not have a folder matching the name of the folder defined in the subaddress, then the subaddress will be treated as an unknown email address and handled accordingly, based on your other MDaemon settings. For example, if `bill.farmer@example.com` does not have a folder named "`stuff`" and yet a message arrives for "`bill`.

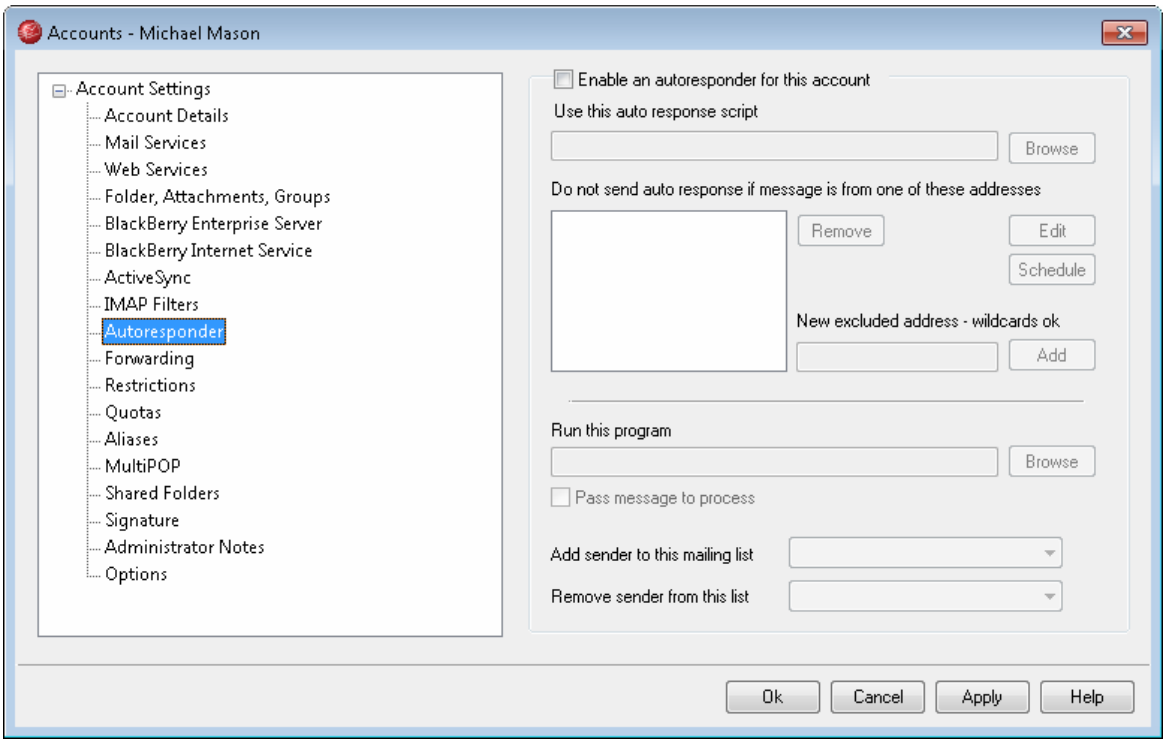
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

farmer+stuff@example.com" then that message will be treated as if were addressed to an unknown user, and it will most likely be rejected.

**Enable subaddressing**
Click this checkbox if you wish to permit subaddressing for this account.

By default, each account has the subaddressing feature disabled. You can, however, disable this feature globally via the *Disable subaddressing feature for all accounts* option located on the Miscellaneous 202 screen of the Preferences dialog. If Subaddressing is disabled via that option, it will not be permitted for any account, regardless of the individual account settings.

### 6.1.1.9 Autoresponder




Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with web access 346 to WorldClient 111 or WebAdmin 132 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

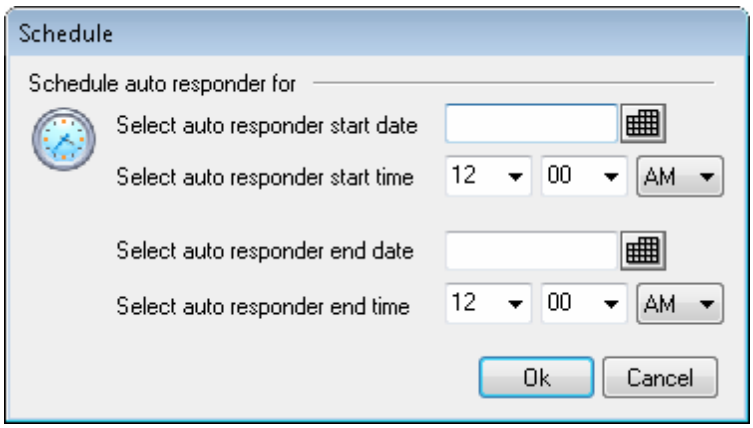
messages are based on response scripts (*.RSP files), which support a large number of macros. These macros can be used to cause much of the script's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating locally, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Options 392 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

**Enable an autoresponder for this account**
Enable this control to activate an autoresponder for the account. For more information on autoresponders see: Autoresponders 390.

**Use this auto response script**
This field is used to specify the path and filename of the response file (*.RSP) that will be processed and used to compose the message that will be returned to the message sender. Response scripts may contain macros that can be used to make response messages dynamic and automate much of their content. See, Creating Auto Response Scripts 393 for more information.

**Schedule**
Click this button to open the Schedule dialog on which you can set a start and end date and time for the Autoresponder to be active. Leave the Schedule blank if you want the Autoresponder to be active continually.




**Do not send auto response if message is from one of these addresses**
Here you can list addresses that you wish to be excluded from responses initiated by this autoresponder.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Occasionally auto response messages may be sent to an address that returns an auto response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. If you encounter one of those addresses, enter it here to prevent that from happening. There is also an option located on the Autoresponders » Options 392 screen, which can be used to limit auto response messages to one response per sender per day.

**Remove**
Click this button to delete any selected entries from the list of excluded addresses.

**New excluded address—wildcards okay**
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

**Edit**
Click this button to open and edit your selected Auto Response Script.

### Run a Program

**Run this program**
Use this field to specify the path and filename to a program that you wish to run when new mail arrives for this account. Care must be taken to ensure that this program terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

**Pass message to process**
Select this option and the process specified in the *Run this Program* field will be passed the name of the triggering message as the first available command line parameter. When the autoresponder is set for an account that is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see Forwarding 362 ) then this function will be disabled.

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible: `logmail /e /j /message=$MESSAGE$ /q`.

### Mailing Lists

**Add sender to this mailing list**
If a mailing list is entered in this field then the sender of the incoming message will be automatically added as a member of that mailing list. This is a handy feature for

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

building lists automatically.

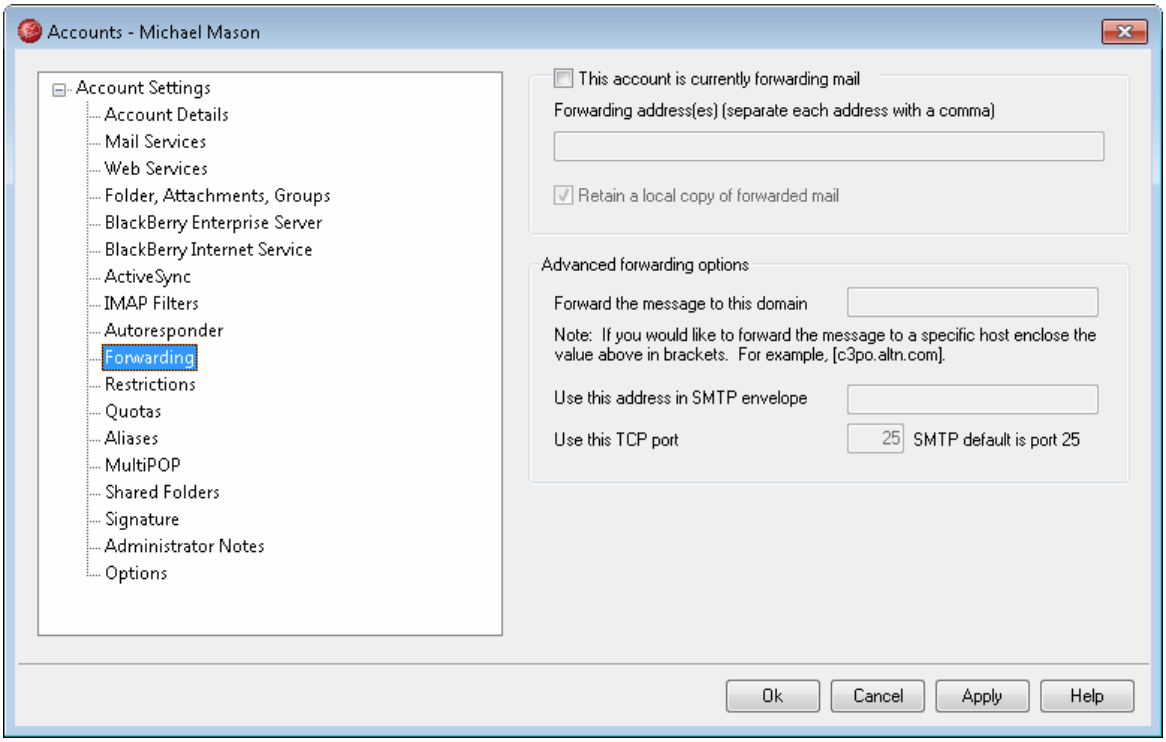
**Remove sender from this mailing list**
If a mailing list is entered in this field then the sender of the incoming message will be automatically added removed from the specified mailing list.

---

**See:**

**Autoresponders » Accounts** 390
**Autoresponders » White List** 391
**Autoresponders » Options** 392
**Creating Auto Response Scripts** 393

### 6.1.1.10 Forwarding




#### Mail Forwarding Options

**This account is currently forwarding mail**
Check this box if you wish to forward this account's incoming messages to the address or addresses specified in the *Forwarding addresses* option below. MDaemon users with web access 346 to WorldClient 111 or WebAdmin 132 can use the options provided to set the forwarding options for themselves rather than requiring an administrator to do so.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Forwarding addresses (separate each address with a comma)**
Use this field to designate any email addresses to which you wish to forward copies of this account's incoming messages as they arrive. A copy of each new message arriving at the server will be automatically generated and forwarded to the addresses specified in this field, provided the *This account is currently forwarding mail* option above is checked. When forwarding to multiple addresses, separate each one with a comma.

**Retain a local copy of forwarded mail**
By default, a copy of each forwarded message is delivered normally to the local user's mailbox. If you uncheck this box then no local copy will be retained.

## Advanced Forwarding Options

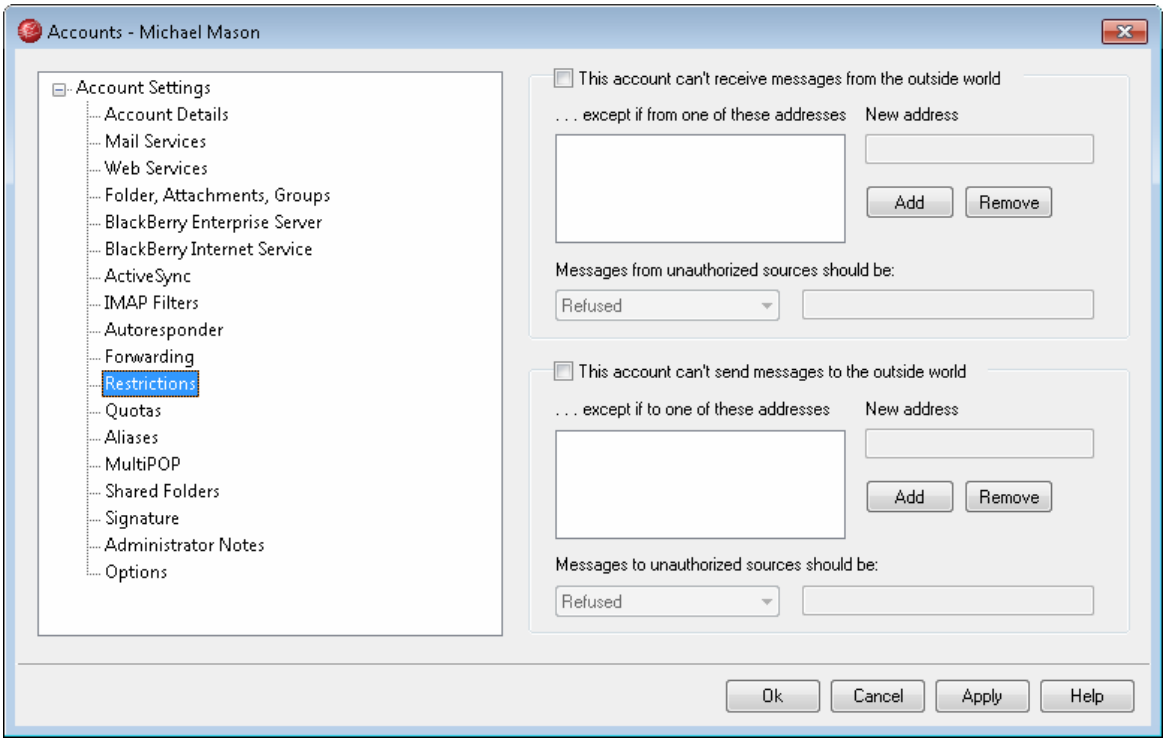
**Forward the message to this domain**
If you wish to route the forwarded messages through a particular domain's MX servers, then specify that domain here. If you wish to route the messages to a specific host, then enclose the value in brackets (e.g. `[host1.example.com]`).

**Use this address in SMTP envelope**
If an address is specified here, it will be used in the "`MAIL From`" statement sent during the SMTP session with the accepting host, instead of using the actual sender of the message. If you require an empty SMTP "`MAIL From`" statement (i.e. "`MAIL FROM <>`") then enter "[trash]" into this option.

**Use this TCP port**
MDaemon will send the forwarded messages using the TCP port specified here. The default SMTP port is 25.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.1.1.11 Restrictions




Use the options on this screen to govern whether or not the account will be able to send or receive mail to or from non-local domains. The *Restrict accounts to sending and receiving local mail only* option on the Mailbox 380 screen of New Account Defaults can be used to apply this restriction to all accounts by default.

#### Inbound Mail Restriction

**This account can't receive messages from the outside world**
Click this checkbox if you want this account to be prevented from receiving email messages from non-local domains.

**...except if from one of these addresses**
Addresses specified in this area are exceptions to the Inbound Mail restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then all inbound messages from any address at altn.com would be accepted and delivered to the account.

**New address**
If you wish to add an address exception to the Inbound Mail Restrictions list then type it here and click the add button.

**Add**
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Remove**
If you wish to remove an address from the restrictions list, select the address and then click this button.

**Messages from unauthorized sources should be...**
The options in this drop-down list box govern what MDaemon will do with messages that are destined for this account but originate from a non-local or otherwise unauthorized domain. You may choose any of the following options:

*Refused* – Restricted messages will be refused by MDaemon.

*Returned to sender* – Messages from restricted addresses will be returned to the sender.

*Sent to postmaster* – Messages that are restricted will be accepted but delivered to the postmaster instead of this account.

*Sent to...* – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

## Outbound Mail Restriction

**This account can't send messages to the outside world**
Click this checkbox if you want the account to be prevented from sending email messages to non-local domains.

**...except if to one of these addresses**
Addresses specified in this area are exceptions to the Outbound Mail restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then all outbound messages to any address at altn.com would be delivered normally by MDaemon.

**New address**
If you wish to add an address exception to the Outbound Mail Restrictions list then type it here and click the add button.

**Add**
After entering an address into the *New address* option, click this button to add it to the exceptions list.

**Remove**
If you wish to remove an address from the restrictions list, select the address and then click this button.

**Messages to unauthorized sources should be...**
The options in this drop-down list box govern what MDaemon will do with messages that originate from this account but are destined for a non-local or otherwise unauthorized domain. You may choose any of the following options:

*Refused* – Messages to unauthorized addresses will be refused by MDaemon.

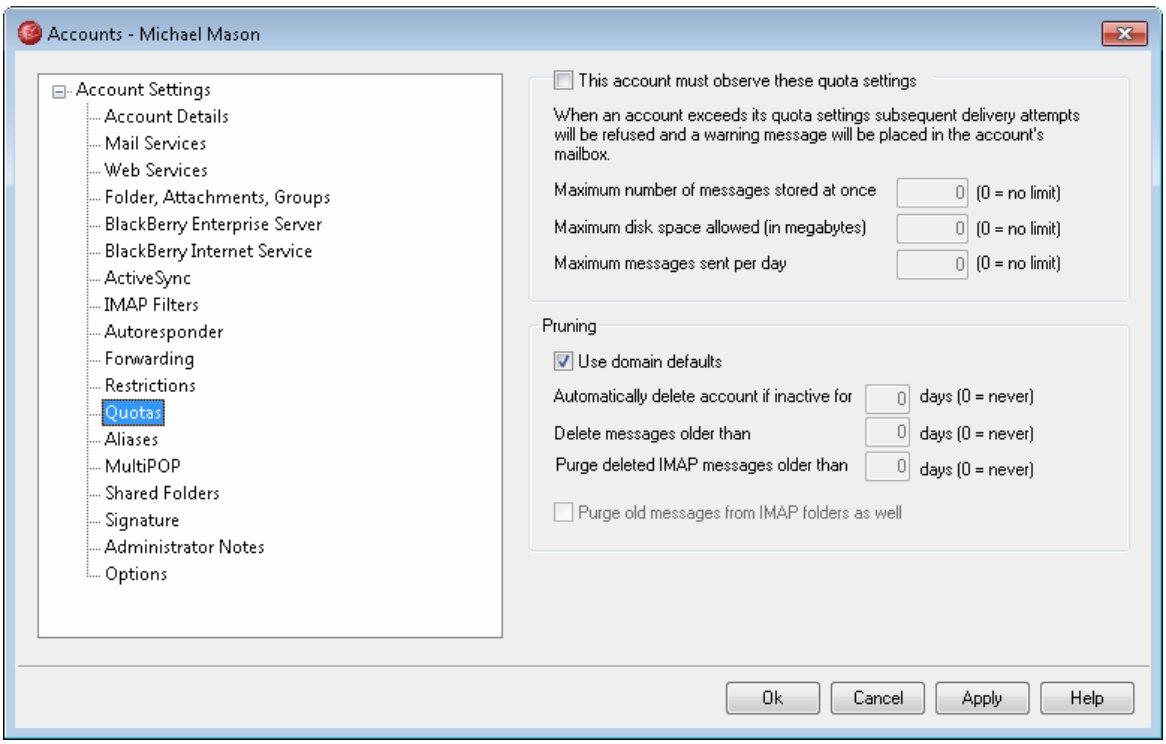
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*Returned to sender* – Messages to restricted addresses will be returned to the sender.

*Sent to postmaster* – Messages that are restricted will be accepted but delivered to the postmaster instead of the designated recipient.

*Sent to...* – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

### 6.1.1.12 Quotas




#### Quota Options

**This account must observe these quota settings**
Check this box if you wish to specify a maximum number of messages that the account can store, set a maximum amount of disk space that the account can use (including any file attachments in the account's `\Files\` folder), or designate a maximum number of messages that the account can send via SMTP per day. If a mail delivery is attempted that would exceed the maximum message or disk space limitations, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP 369 collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Use the *Accounts that exceed this percent of their quota will be warned* option at "Accounts » Account Settings » Quotas 385" to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message.

**Maximum number of messages stored at once**
Use this option to designate the maximum number of messages that can be stored for the account. Using "0" in the option means there will be no limit to the number of messages permitted.

**Maximum disk space allowed (in megabytes)**
Use this option to designate the maximum amount of disk space that the account can use, including any file attachments that may be stored in the account's `\Files\` folder. Using "0" in the option mean there will be no limit to the amount of disk space that the account can use.

**Maximum messages sent per day**
Use this option to designate the maximum number of messages that the account can send per day via SMTP. If the account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages the account can send.

## Pruning

The options in this section are used to designate when or if this account will be deleted by MDaemon if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain amount of time. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit.

**Use domain defaults**
The default Pruning settings are domain-specific and located at: Default Domain/ Servers » Pruning 61 and Domain Manager 108. If you wish to override the domain defaults for this account, clear this checkbox and set the desired values in the options below.

**Automatically delete account if inactive for [XX] days (0 = never)**
Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account will never be deleted due to inactivity.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Delete messages older than [XX] days (0 = never)**
This is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

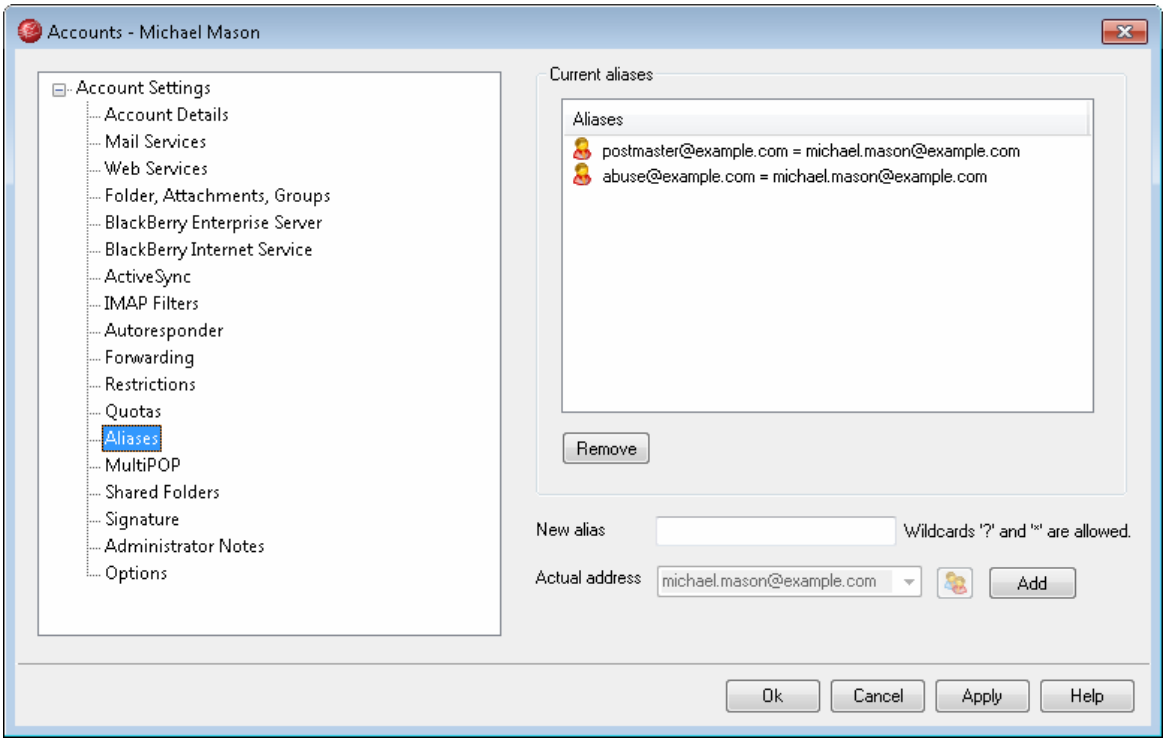
**Purge deleted IMAP messages older than [XX] days (0 = never)**
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

**Purge old messages from IMAP folders as well**
Click this checkbox if you want the "*Delete messages older than...*" option to apply to messages in IMAP folders as well. When this option is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

**See:**

**New Account Defaults » Quotas** 385
**Account Settings » Quotas** 419

### 6.1.1.13 Aliases




This screen lists all address aliases 398 associated with the account, and can be used

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

to add or remove them.

### Removing an Alias

To remove an alias from the account, select the alias in the list and then click **Remove**.

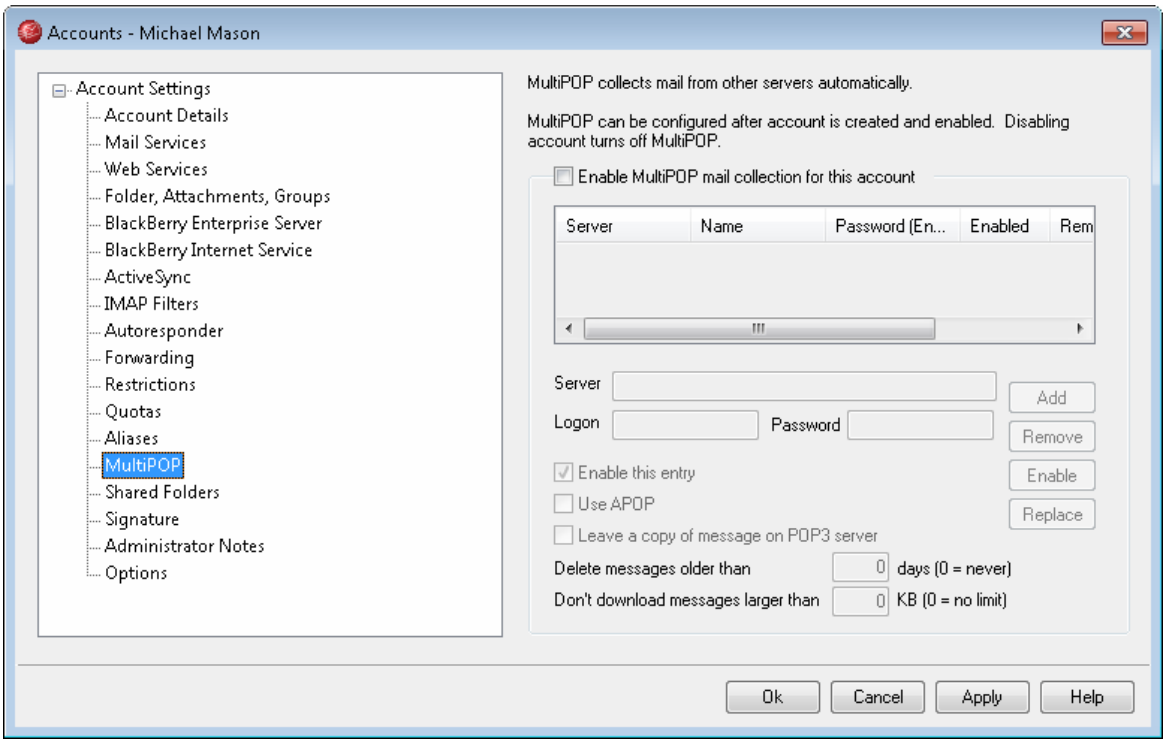
### Adding an Alias

To add a new alias to the account, in the *New alias* box type the address that you wish to associate with the account and then click **Add**. The wildcards "?" and "*" are permitted, representing single characters and single words, respectively.

**See:**

**Address Aliases** 398

## 6.1.1.14 MultiPOP




The MultiPOP feature allows you to create an unlimited number of POP3 host/user/password combinations for collection of mail messages from multiple sources. This is useful for your users who have mail accounts on multiple servers but would prefer to collect and pool all their email together in one place. Before being placed in the user's mailbox, MultiPOP collected mail is first placed in the local queue so that it can be processed like other mail having Autoresponders and Content filters applied to it. The

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

scheduling options for MultiPOP are located at: Setup » Event Scheduling » Mail Scheduling Options » MultiPOP Collection 150.

**Enable MultiPOP mail collection for this account**
Check this box to enable MultiPOP processing for this account.

**MultiPOP host list for this account**
This box contains the list of all MultiPOP host entries that have been created for this account.

### Creating or Editing a MultiPOP Entry

**Server**
Enter the POP3 server from which you wish to collect mail.

**Logon**
Enter the POP3 username or login name that is associated with the mail account on the server specified above.

**Password**
Enter the POP3 or APOP password used for accessing the mail account on the specified server.

**Use APOP**
Click this checkbox if you want the MultiPOP entry to use the APOP method of authentication when retrieving mail from its corresponding host.

**Leave a copy of message on POP3 server**
Click this checkbox if you want to leave a copy of collected messages on the server. This is useful when you plan to retrieve these messages again at a later time from a different location.

**Delete messages older than [XX] days (0 = never)**
This is the number of days that a message can remain on the MultiPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

**Don't download messages larger than [XX] KB (0 = no limit)**
Enter a value here if you wish to limit the size of messages that may be downloaded.

**Add**
After entering all of the information for the new MultiPOP entry, click this button to add it to the list.

**Remove**
If you wish to delete one of your MultiPOP entries, select the desired entry and then click this button.

**Enable/disable**
Clicking this button toggles the state of the selected MultiPOP entries. This switch

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

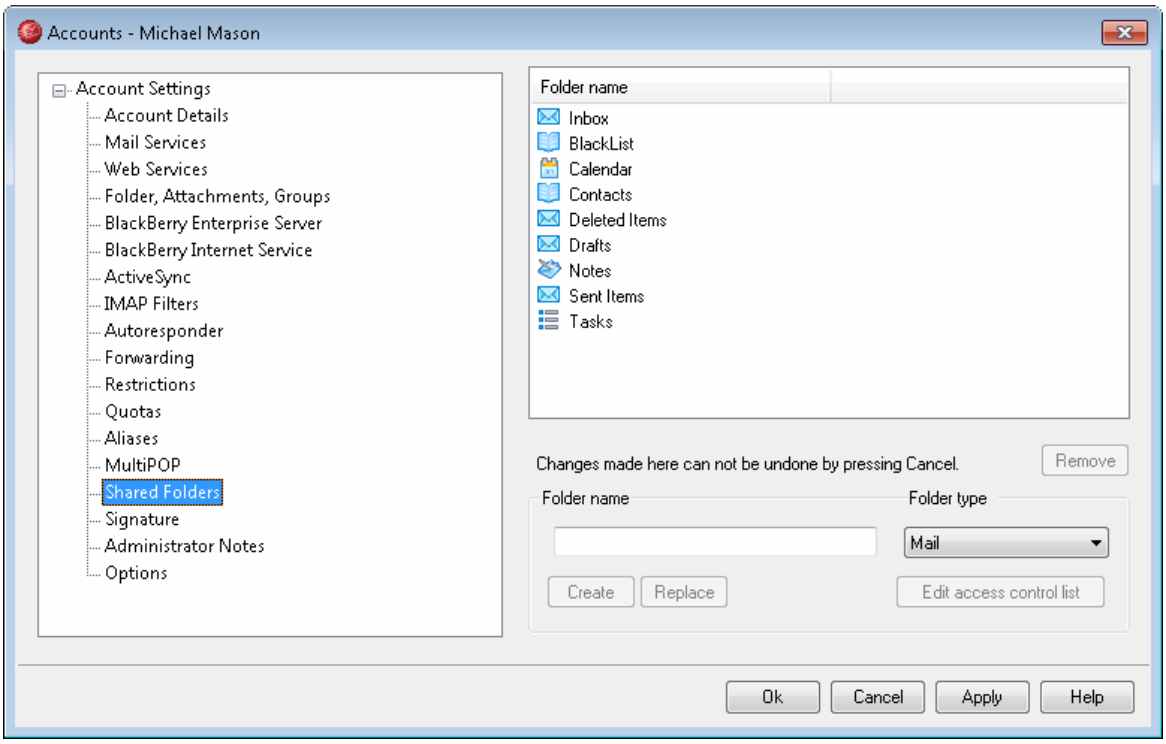
gives you control over whether MDaemon will collect mail for this entry or skip over it when it performs its MultiPOP processing.

**Replace**
To edit an entry, click the desired entry in the list, which will then have its settings displayed in the options on this screen. After making any changes, click this button to apply those changes to the entry.

**See:**

**Event Scheduling » MultiPOP Collection** 150

### 6.1.1.15 Shared Folders




This screen is only available when the *Enable shared folders* option is enabled on the Public & Shared Folders 75 screen, located at Setup » Default Domain/Server » Public & Shared folders.

**IMAP Folders**

This top section displays all of the user's IMAP Folders and can be used to share access to them with other MDaemon users or Groups. When the account is first created, this area will only have the Inbox listed until you use the *Folder name* and *Create* options (or the options on Filters 356) to add folders to it. Subfolders in this

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

list will have the folder and subfolder names separated by a slash.

**Remove**
To remove a Shared IMAP folder from the list, select the desired folder and then click the *Remove* button.

**Folder name**
To add a new folder to the list, specify a name for it in this option and click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, then prefix the new folder's name with the parent folder's name and a slash. For example, if the parent folder is "My Folder" then the new subfolder name would be "My Folder/My New Folder". If you don't want it to be a subfolder then name the new folder "My New Folder" without the prefix.

**Folder type**
Use this drop-down list to choose the type of folder you wish to create: Mail, Calendar, Contacts, and so on.

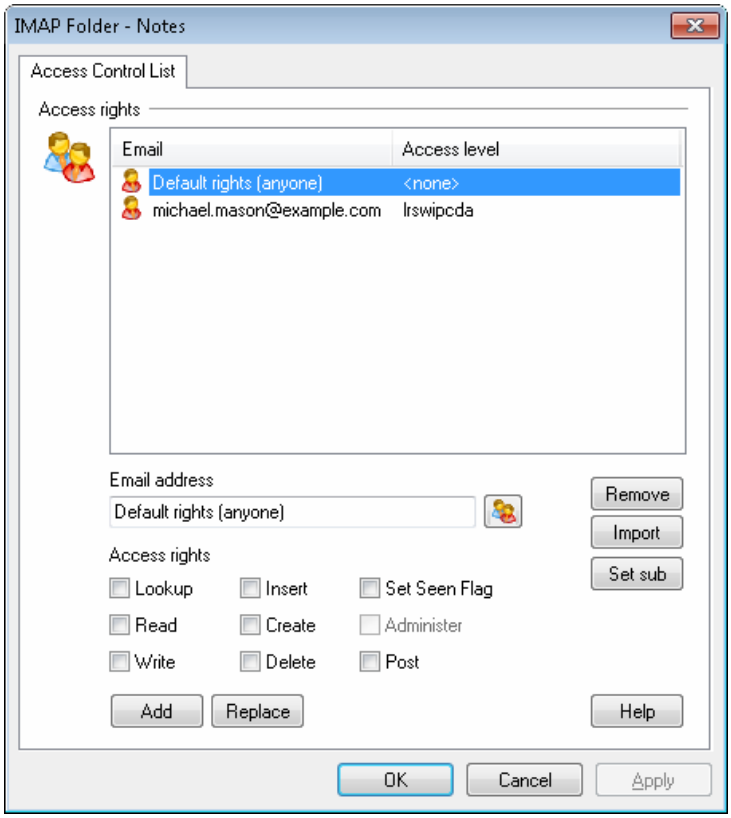
**Create**
After specifying a folder's name click this button to add the folder to the list.

**Replace**
If you wish to edit one of the Shared Folders, click the entry, make the desired change, and then click *Replace.*

**Edit access control list**
Choose a folder and then click this button to open the Access Control List 373 dialog for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.1.1.15.1 Access Control List




#### Access Rights

This area is for designating the MDaemon user accounts or groups that you wish to grant access to the shared folder, and for setting the access permissions for each one. You can reach this dialog from the Shared Folders 371 screen of the Account Editor. Double-click the desired folder, or click the folder and then click *Edit access control list*, to open the Access Control List for that folder. Each entry lists the email address of the account and a one letter Access Level abbreviation for each Access Right that you grant to the user.

**Email address**
Type the email address or click the Account icon to choose the MDaemon account or group that you wish to grant access to the shared folder. After designating an account or group, choose the desired Access Rights and then click *Add* to add that entry to the list.

**Remove**
To remove an entry from the Access Rights list, select the desired entry and then click *Remove*.

**Import**
With the *Import* feature you can add the members of an existing Mailing List to the list of users with Access Rights. Choose the access rights that you wish to grant to the users, click Import, and then double-click the desired list. All of the list's

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

members will be added to the list with the rights that you set.

**Set sub**
Click *Set sub* if you wish to copy this folder's access control permissions to any subfolders it currently contains.

### Access Rights

Choose the rights that you wish to grant to the user or group by clicking the desired options in this area and then clicking *Add* for new entries or *Replace* for existing entries.

You can grant the following Access Control Rights:

**Lookup (l)** – user can see this folder in their personal list of IMAP folders.

**Read (r)** – user can open this folder and view its contents.

**Write (w)** – user can change flags on messages in this folder.

**Insert (i)** – user can append and copy messages into this folder.

**Create (c)** – user can create subfolders within this folder.

**Delete (d)** – user can delete messages from this folder.

**Set Seen Flag (s)** – user can change the read/unread status of messages in this folder.

**Administer (a)** – user can administer the ACL for this folder.

**Post (p)** – user can send mail directly to this folder (if folder allows).

**Add**
After designating an Email Address or Group and choosing the access rights that you wish to grant, click *Add* to add the account or group to the list.

**Replace**
To modify an existing Access Rights entry, select the entry, make any desired changes to the Access Rights, and then click *Replace*.

**Help**
Click *Help* to display a list of the access rights and their definitions.

Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting access rights to your folders to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at:

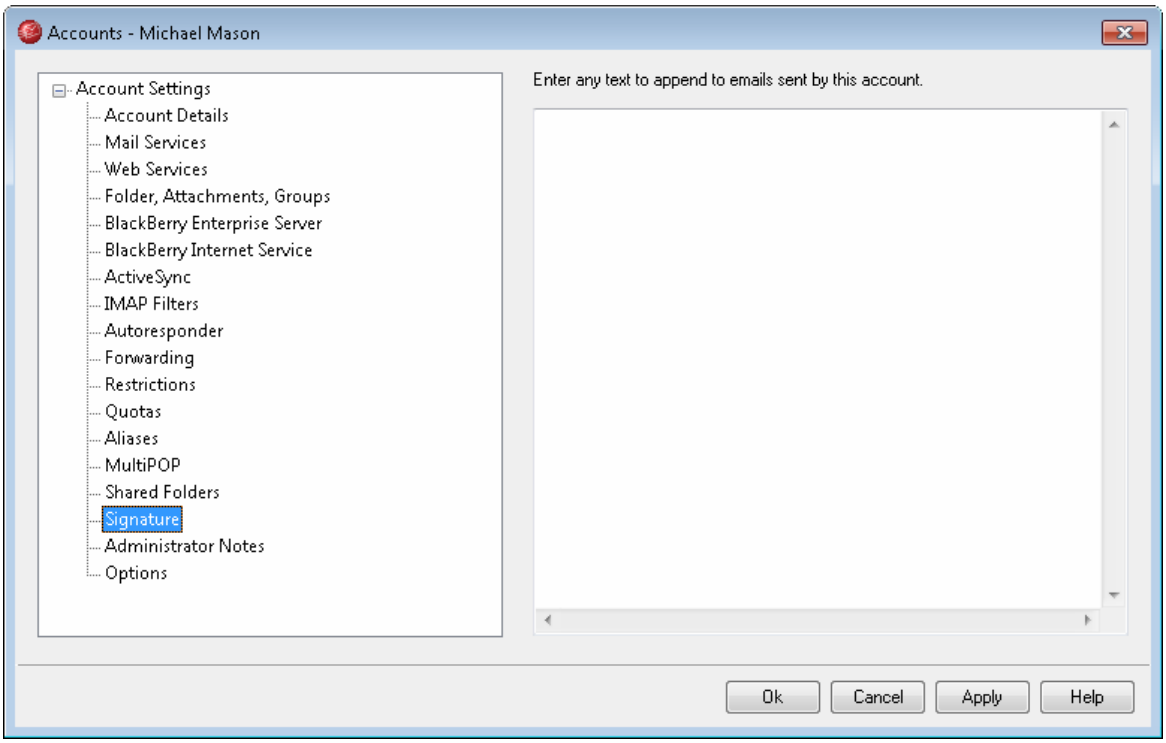
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

http://www.rfc-editor.org/rfc/rfc2086.txt.

**See:**

**Account Editor » Shared Folders** 371
**Public & Shared Folders** 75
**Folder Listing** 77

### 6.1.1.16 Signature



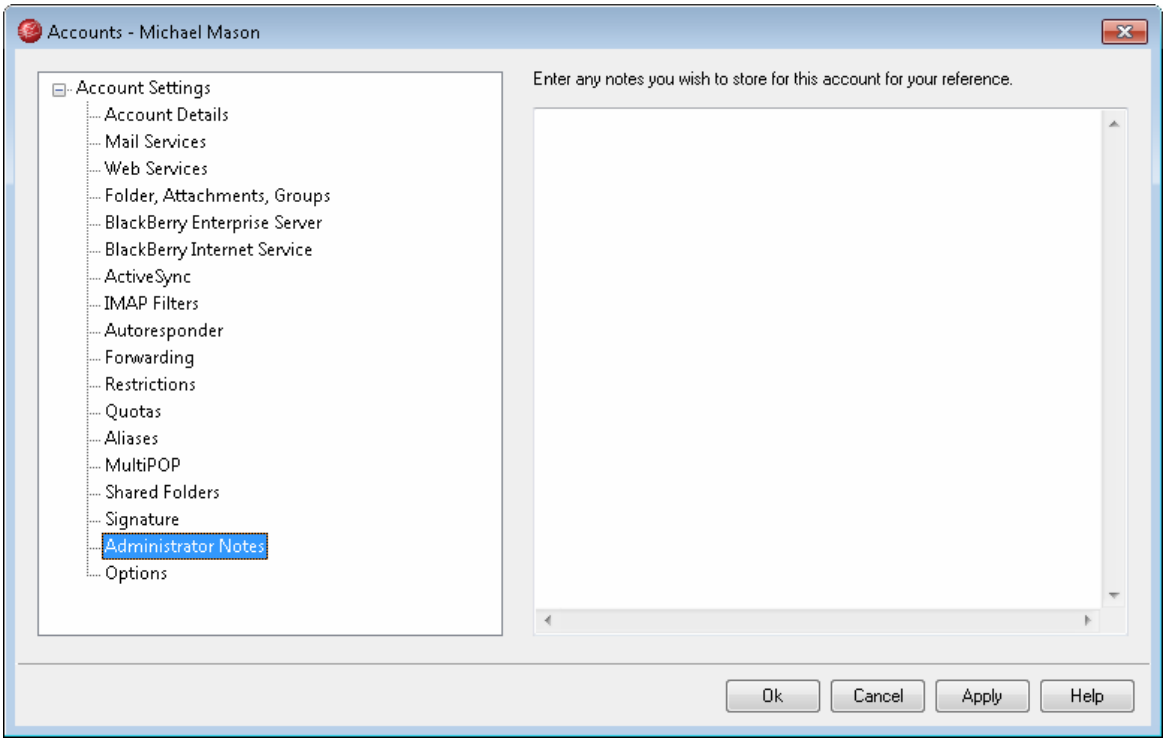

**Account Signature**

Use this screen to designate a signature that will be appended to the bottom of every email that the account sends. This signature is added in addition to any other signatures or footers added by other options, such as the signature option included in WorldClient and other mail clients, the Domain Signatures 72 option, and Mailing List footers 445. Domain Signatures and Mailing List footers are always added below Account Signatures.

Users with access to WebAdmin 132 can edit their own signatures via the My Account » Signature options included there.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

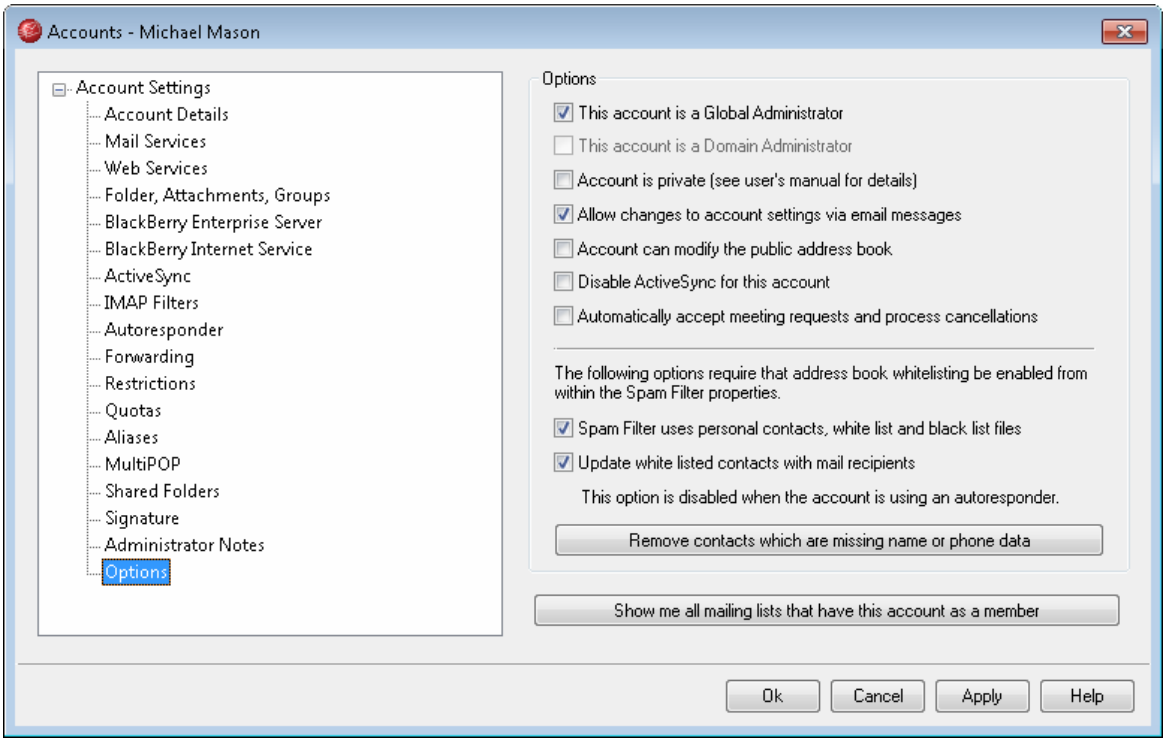
### 6.1.1.17 Administrator Notes




Use this screen for any notes or other information you wish to save for your own reference regarding this account. Unlike the *Description* field on the Account Details 343 screen, Administrator Notes will not be synchronized to the public contacts or mapped to any field in Active Directory.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.1.1.18 Options




#### Options

**This account is a Global Administrator**
Enable this checkbox to grant the user server-level administrative access. Global Administrators have:

- Full access to server configuration, all users, and all domains via WebAdmin
- Access to all MDaemon users of all MDaemon domains as Instant Messaging buddies.
- The ability to post to all mailing lists even if flagged as "Read Only".
- The ability to post to all mailing lists even if not a member.

The user will have complete access to MDaemon's files and options. For a discussion on the administrative options within WebAdmin, see the WebAdmin section.

**This account is a Domain Administrator**
Click this checkbox to designate the user as a Domain Administrator. Domain Administrators are similar to Global Administrators except that their administrative access is limited to the domain to which they belong. For more information on Domain Administrators see the WebAdmin section.

**Account is private**
MDaemon automatically creates and maintains an "everyone@" mailing list for each domain, which can be used to send a message to everyone at once. By default MDaemon will include all accounts when it constructs this list. Check this box if you

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

wish to exclude this account from that list. This will also hide the account from shared calendars and VRFY[46] results. The account's address book entry will not be hidden, however, from a global address book lookup performed on a BlackBerry device that is activated on your MDaemon's BlackBerry Enterprise Server.

**Allow changes to account settings via email messages**
When this option is enabled, the user will have access to account-related commands that can be included in specially formatted email messages sent to the server. This feature allows the user to perform common account maintenance tasks such as changing his name, password, forwarding options, and so on. For a complete discussion on remote account manipulation via email messages, see: Remote Server Control Via Email[504].

**Account can modify the public address book**
Click this option if you want the account to be able to add and delete entries from the WorldClient or LDAP-based public address books.

If the Account is synchronizing folders with ComAgent then modifications could be propagated to all users. Exercise caution when enabling this feature.

**Disable ActiveSync for this account**
Check this box if you wish to disable ActiveSync for the account. The user will not be able to use ActiveSync on a mobile device to synchronize his or her contacts and calendar data with MDaemon/WorldClient.

**Automatically accept meeting requests and process cancellations**
Click this checkbox if you wish to cause automatic processing of meeting requests, changes, and cancellations for this account. When the account receives a message that contains a meeting request, the account's calendar will be updated automatically. This option is disabled for all accounts by default.

**Spam Filter uses personal contacts, white list, and black list files**
The Spam Filter's White List (automatic)[253] screen contains a global option that can be used to cause the Spam Filter to white list a message automatically when the sender of the message is found in the local recipient's personal contacts or white list files. It will also automatically black list a message when the sender is found in the user's black list file. If you have enabled the Spam Filter's global option but do not wish to apply it to this account, clear this check box to override the global setting. If the global option is disabled then this option will not be available.

**Note:** Keeping your contacts updated and synchronized with WorldClient, the Windows Address Book, and other MAPI mail clients that use the Windows Address Book can be easily done using ComAgent[114].

**Update white listed contacts with mail recipients**
Click this option if you wish to update this account's white list folder each time it sends an outgoing message to a non-local email addresses. When used in conjunction with the above option, *Spam Filter uses personal contacts, white list, and black list files*, the number of Spam Filter false positives can be drastically

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

reduced. The *Automatically update white listed contacts* option located on the White List (automatic) 253 screen must be enabled before you can use this feature.

**Note:** This option is disabled when the account is using an autoresponder.

**Remove contacts which are missing name or phone data**
Click this button if you wish to remove every contact that contains only an email address from the account's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who have been using MDaemon's automatic white listing option prior to version 11 purge contacts that were added purely as a function of the white list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated white list folder. This could result in the account having many entries in the contacts folder that the user would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

**Show me all mailing lists that have this account as a member**
Click this button to open a list of all Mailing Lists 430 that have this account as a member.

**See:**

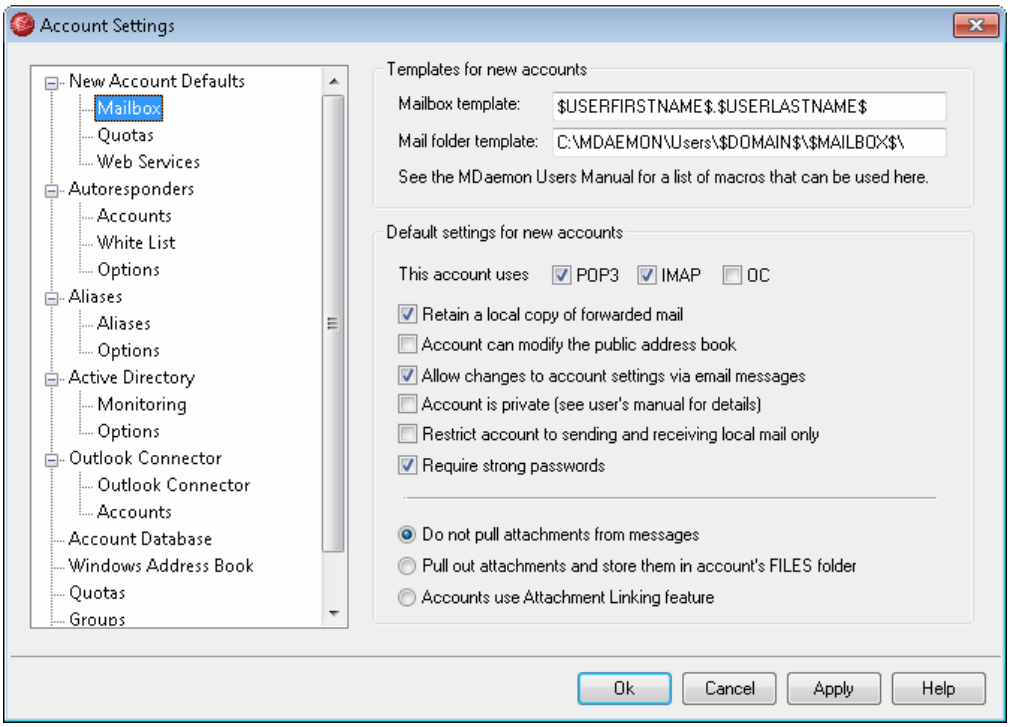
**White List (automatic)** 253

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# 6.2 Account Settings

## 6.2.1 New Account Defaults

### 6.2.1.1 Mailbox




The options on this dialog make it possible for you to specify the default values for various common account settings located on the Account Editor[343]. Further, the *Mailbox template* and *Mail folder template* make it possible for you to use a variety of special macros[383] to automatically generate the email address and mail storage folder whenever an account is created or imported. Use of these templates can greatly simplify and automate new account management.

**Templates for new accounts**

**Mailbox template**
Use this field to specify a default Mailbox name template for new accounts. In addition to being the Mailbox, this value will be the name passed in the `USER` POP3 command, which enables access to a mailbox from a remote location or POP aware mail clients. See Template Macros[383] for a list of the Macros that can be used in this template string. "`$USERFIRSTNAME$.$USERLASTNAME$`" is the default template for this option. So, creating an account for "Michael Mason" under the example.com domain would result in his mailbox being set to "`Michael.Mason@example.com`".

**Mail folder template**
Use this field to specify a default mail folder template for new accounts. Each account's *Mail folder* is where its email messages will be stored on the server. Care must be taken to ensure that once expanded, the template provided here will form a

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

valid file path.

MDaemon supports a basic system for folder hashing. Under NTFS, keeping many folders under the same root can cause performance problems. To reduce this problem you can use the macro `$MAILBOXFIRSTCHARSn$` where "n" is a number between 1 and 10. This will expand to the first "n" characters of the mailbox name. Changing your default mail directory template to something like the following will achieve a decent folder hashing system:

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\.
```

### Default settings for new accounts

These options are used for designating default values for various account settings. For more information on these options, see the Account Editor 343.

#### This account uses...

**POP3**
By default accounts can access their email via POP3 mail clients. Clear this checkbox if you do not wish to allow POP3 access to new accounts by default. This option determines the default setting of the POP3 option located on the Account Editor's Account Details 343 screen.

**IMAP**
By default accounts can access their email via IMAP mail clients. Clear this checkbox if you do not wish to allow IMAP access to new accounts by default. IMAP support is only available in MDaemon PRO. This option determines the default setting of the IMAP option located on the Account Editor's Account Details 343 screen.

**OC**
Check this box if you wish to allow new accounts to use Outlook Connector 408. This option corresponds to the *Account can use Outlook Connector v2.x* option on the Mail Services 345 screen of the Account Editor.

**Retain a local copy of forwarded mail**
By default MDaemon will retain a local copy of each incoming message in the user's mailbox when his or her account is set to forward mail. This option determines the default setting of the corresponding option located on the Account Editor's Forwarding 362 screen.

**Account can modify the public address book**
This option determines the default setting of the corresponding option located on the Account Editor's Options 377 screen. Click this option if you want new accounts to be able to add and delete entries from the WorldClient or LDAP-based public address books.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

If an Account is synchronizing folders with ComAgent then modifications could be propagated to all users. Exercise caution when enabling this feature.

**Allow changes to account settings via email messages**
This option determines the default setting of the corresponding option located on the Account Editor's Options 377 screen. When this option is enabled, new users will have access to account-related commands that can be included in specially formatted email messages sent to the server. This feature allows the user to perform common account maintenance tasks such as changing his name, password, forwarding options, and so on. For a complete discussion on remote account manipulation via email messages, see: Remote Server Control Via Email 504.

**Account is private**
This option determines the default setting of the corresponding option located on the Account Editor's Options 377 screen. MDaemon automatically creates and maintains an "everyone@" mailing list for each domain, which can be used to send a message to everyone at once. By default MDaemon will include all accounts when it constructs this list. Check this box if you wish to hide or exclude new accounts from that list. This will also hide the accounts from calendars and VRFY 46 results.

**Restrict account to sending and receiving local mail only**
This option determines the default setting of the two options located on the Account Editor's Restrictions 364 screen. If this option is enabled then both the *This account can't receive messages from the outside world* and *This account can't send messages to the outside world* options on that dialog will be enabled for all new accounts. New accounts will be restricted to sending and receiving local mail only.

**Require strong passwords**
By default, MDaemon requires strong passwords when creating new accounts or changing existing passwords. Clear this check box if you wish to disable the strong password restriction by default.

**Strong passwords:**

- Must must contain at least a specified number of characters (six by default).
- Must contain both letters and numbers.
- Must contain both upper and lower case letters.
- May not contain the account mailbox or full name data.

You can designate the minimum password length by editing the following key in `MDaemon.ini`:

```
[Special]
MinPasswordLength=XX (default 6)
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Attachment Handling

The remaining three options correspond to the attachment options located on the Account Editor's Folder, Attachments, Groups 349 page.

**Do not pull attachments from messages**
If this option is selected, by default attachments will not be extracted from the account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

**Pull out attachments and store them in the account's FILES folder**
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages. Extracted files are removed from the incoming message, decoded, and placed in the account's `\Files\` subfolder. A note is then placed within the body of the message, listing the names of the files that were extracted. This option does not provide a link to the stored attachments, therefore the user would need the appropriate network access rights to retrieve them. The level of security and user requirements for getting to these files is up to you and depends entirely upon your particular system and the security measures that you have implemented.

**Accounts use Attachment Linking feature**
This option causes attachments to be extracted from the account's incoming messages and stored in the location designated on the Attachment Linking 142 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier that the server uses to map the file to the actual path.

If Attachment Linking is globally disabled on the Attachment Linking 142 dialog, attachments will not be extracted from messages, regardless of the setting selected here.

**See:**

**Template Macros** 383
**Account Editor** 343
**Folder, Attachments, Groups** 349
**Attachment Linking** 142

## 6.2.1.1.1 Template Macros

Below is a quick reference to the macros available for automating your account setup.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

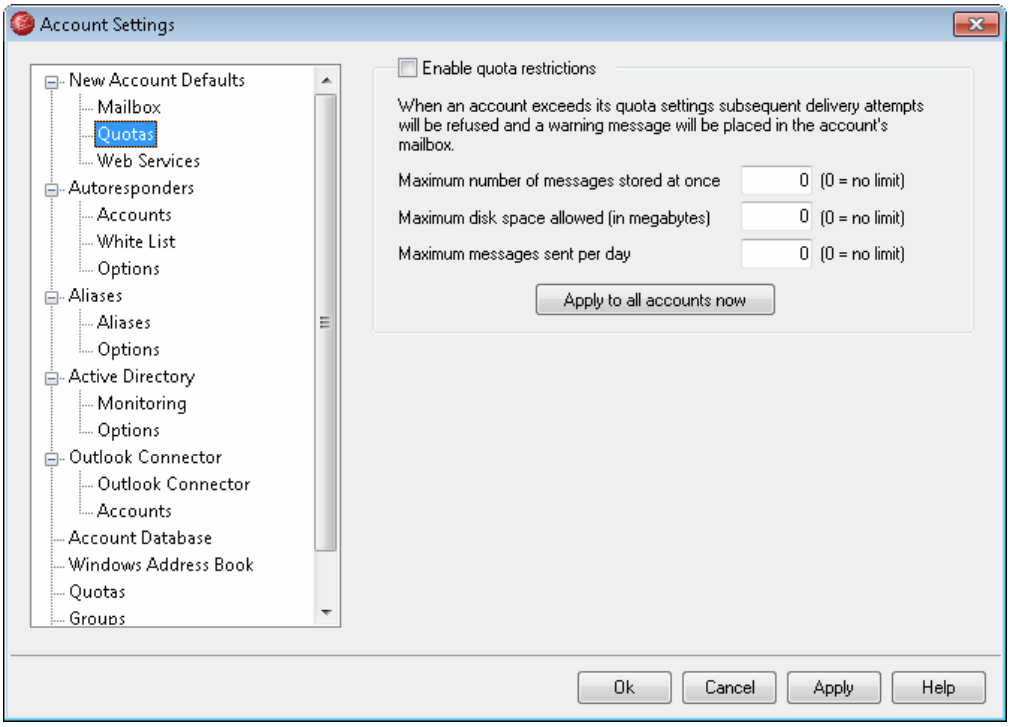
| | |
|---|---|
| $DOMAIN$ | This variable will resolve to the domain name selected for the account. |
| $DOMAINIP$ | This variable will resolve to the IP associated with the domain currently selected for the account. |
| $MACHINENAME$ | This macro returns the machine name field from the Domain tab of the Default Domain dialog. The macro is now used in the default account information script (NEWUSERHELP.DAT) for new installations. |
| $USERNAME$ | This variable resolves to the full first and last name of the account holder. This field is equivalent to "$USERFIRSTNAME$ $USERLASTNAME$" |
| $USERFIRSTNAME$ | This variable resolves to the first name of the account holder. |
| $USERLASTNAME$ | This variable resolves to the last name of the account holder. |
| $USERFIRSTINITIAL$ | This variable resolves to the first letter of the account holder's first name. |
| $USERLASTINITIAL$ | This variable resolves to the first letter of the account holder's last name. |
| $MAILBOX$ | This variable resolves to the mailbox name of the current account. The value will also be used as the value of the USER command passed during POP3 mail sessions. |
| $MAILBOXFIRSTCHARSn$ | Where "n" is a number between 1 and 10. This will expand to the first "n" characters of the mailbox name. |

**See:**

**New Account Defaults » Mailbox** 380

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.2.1.2 Quotas




This screen is used for designating the default values for account quota settings. These options correspond to the Quotas 366 settings on the Account Editor.

#### Quotas

**Enable quota restrictions**
Check this box if you wish to set quotas for all new accounts. You can specify a maximum number of messages that accounts can store, set a maximum amount of disk space that accounts can use (including any file attachments in the each account's `\Files\` folder), and designate a maximum number of messages that accounts can send per day. If a mail delivery is attempted that would exceed an account's quota, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP 369 collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Use the *Warning email sent when this percent is reached* option at "Accounts » Account Settings » Quotas 419" to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining. Further, if an existing warning is found in the account's mailbox

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

it will be replaced with an updated message.

**Maximum numbers of messages stored at once**
Use this option to designate the maximum number of messages that can be stored for new accounts. Using "0" in the option means there will be no limit to the number of messages permitted.

**Maximum disk space allowed (in megabytes)**
Use this option to designate the maximum amount of disk space that new accounts can use, including any file attachments that may be stored in each new account's `\Files\` folder. Using "0" in the option mean there will be no limit to the amount of disk space that the accounts can use.

**Maximum messages sent per day**
Use this option to designate the maximum number of messages that new accounts can send per day via SMTP. If an account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages an account can send.

### Apply to all accounts now

Click this button to apply the settings on this screen to all existing MDaemon accounts. This will reset all accounts to the default Quota values.

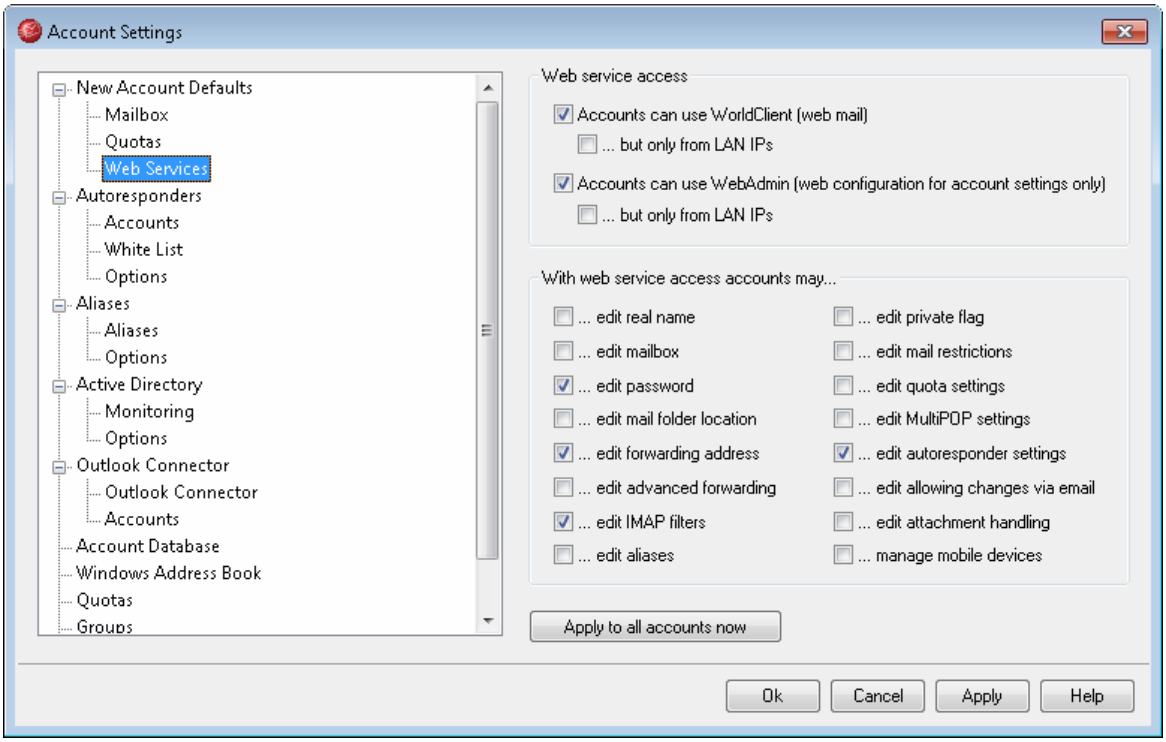
---

**See:**

**Account Editor » Quotas** 366
**Account Settings » Quotas** 419

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.2.1.3 Web Services




The Web Services screen of the New Account Defaults dialog is used for designating the default access rights that new accounts will have for WorldClient 111 and WebAdmin 132. You can designate whether or not accounts will be able to access their email via WorldClient and whether or not users will be able to configure their accounts via WebAdmin. In addition, if you are granting access to WebAdmin, you can control which settings that accounts will be allowed to edit. All of the options on this dialog control the default settings of the corresponding options located on the Account Editor's Web Services 346 screen.

#### Web Service Access

**Account can use WorldClient (web mail)**
Enable this checkbox if you want new accounts to be able to access the WorldClient 111 server, which enables users to check their email using a web browser.

**...but only from LAN IPs**
Check this box if you wish to allow new accounts to access WorldClient only when connecting from a LAN IP address 336.

**Account can use WebAdmin (web configuration for account settings only)**
Check this box if you wish to grant new accounts permission to modify their account settings via WebAdmin 132. Users will only be able to edit those settings that you enable below.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...but only from LAN IPs**
Check this box if you wish to allow new accounts to access WebAdmin only when connecting from a LAN IP address[336].

### With web service access accounts may...

**...edit real name**
Enabling this feature will allow new users to modify their *First and last name* setting.

**...edit mailbox**
Enabling this feature will allow new users to modify the mailbox portion of their *Email address*.

Because the mailbox is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

**...edit password**
Click this checkbox if you wish to allow new users to modify their *Email password.*

**...edit mail folder location**
Checking this box gives each new user permission to modify the account's Message Folder[349].

You should exercise caution in granting this permission to users. Giving users permission to change their message folder effectively gives them the ability to affect any folder on your server.

**...edit forwarding address**
When this feature is enabled, the new user will be able to modify the forwarding[362] address settings.

**...edit advanced forwarding**
When this feature is enabled, the new user will be able to modify the *Advanced Forwarding Options.*

**...edit IMAP filters**
Use this control to enable users to create and manage their own mail filters[356]. This feature is only available in MDaemon PRO.

**...edit aliases**
Enable this option if you wish to allow new accounts by default to use MDaemon's web services to edit Address Aliases[368] associated with their accounts.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...edit private flag**
This option governs whether or not new accounts will be permitted to use WebAdmin to edit the "*Account is private*" option located on the Account Editor's Options 377 screen.

**...edit mail restrictions**
This checkbox controls whether or not new accounts will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions 364 screen.

**...edit quota settings**
Click this checkbox if you wish to allow accounts to modify the quota 366 settings.

**...edit MultiPOP settings**
Click this checkbox if you wish to give the new accounts permission to add new MultiPOP 369 entries and to enable/disable MultiPOP collection for those entries.

**...edit autoresponder settings**
Click this checkbox if you wish to give the users permission to add, edit, or delete Autoresponders 359 for their accounts.

**...edit allow changes via email**
Click this checkbox if you wish to allow new users to modify their *Account Settings* via specially formatted email messages 504.

**...edit attachment handling**
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Folder, Attachments, Groups 349 screen.

**...manage mobile devices**
Use this option if you wish to allow new accounts to use MDaemon's web services to manage their mobile device settings.

### Apply to all accounts now

Click this button to apply the settings on this screen to all existing MDaemon accounts. This will reset all accounts to the default Web Services values. Because it is an irreversible action you should exercise caution before using it.

---

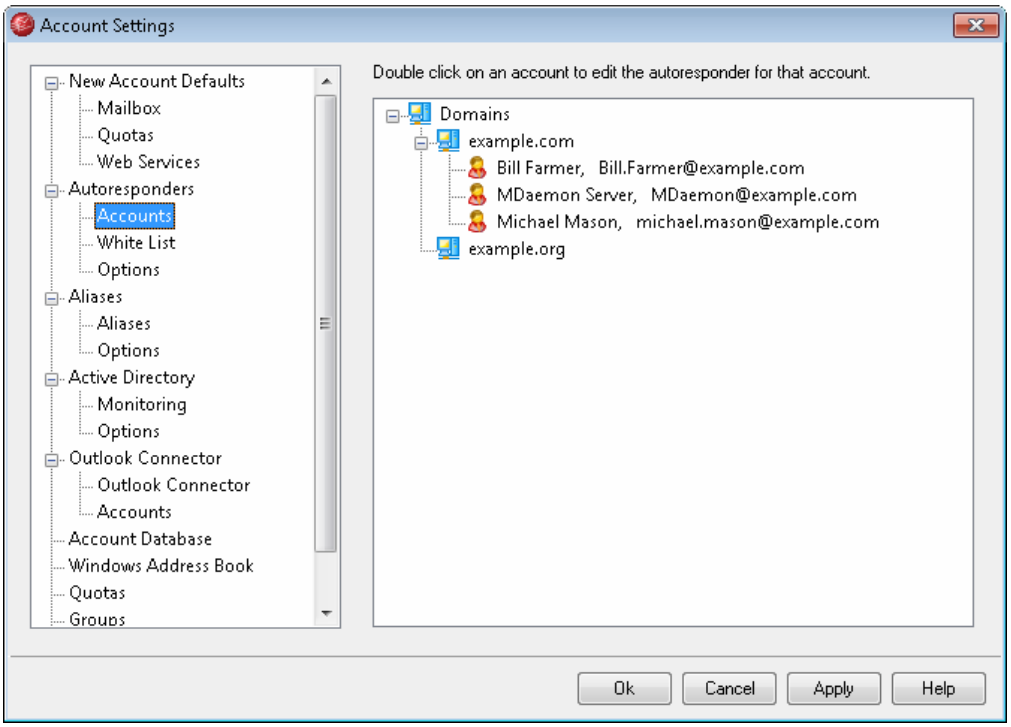
**See:**

**Account Editor » Web Services** 346

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 6.2.2 Autoresponders

### 6.2.2.1 Accounts




Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with Web Access 346 to WorldClient 111 or WebAdmin 132 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Further, accounts with BlackBerry devices activated on MDaemon's BlackBerry Enterprise Server 162 can use the "Out of Office Reply" option under their device's email settings to configure their autoresponder. Finally, automated response messages are based on response scripts ( `*.RSP` files), which support a large number of macros. These macros can be used to cause much of the script's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating locally, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Options 392 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

**Account List**

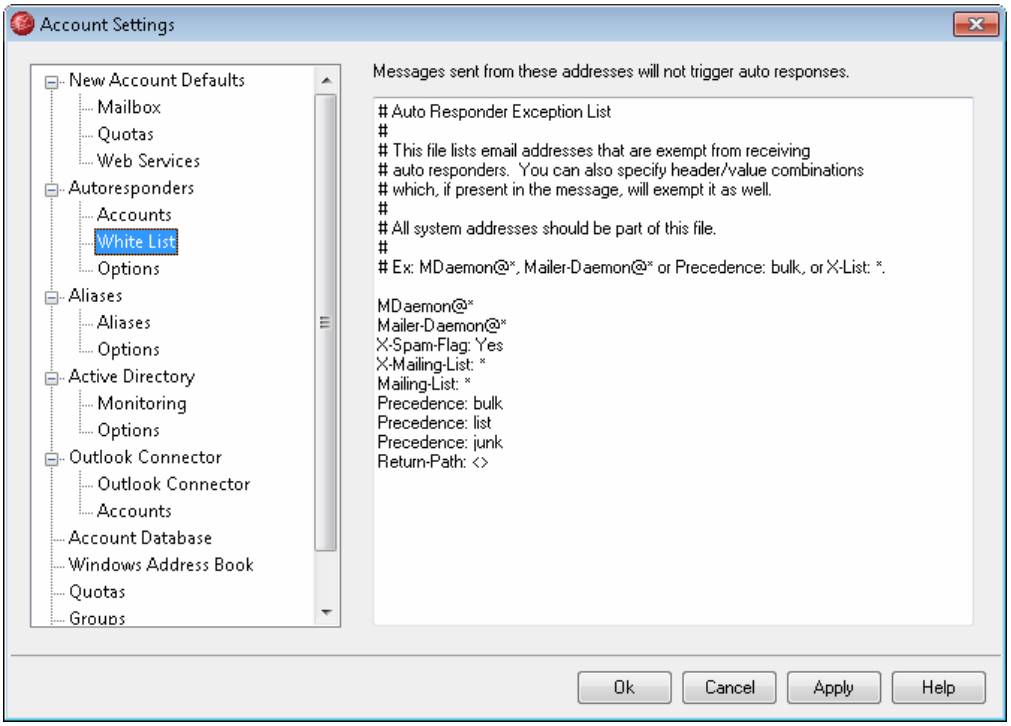
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

This area lists all available local mailboxes that can host an autoresponder. Double-click an account in this list to open its corresponding Autoresponder[359] screen, which is used to configure an autoresponder for that account.

**See:**

**Autoresponders » White List**[391]
**Autoresponders » Options**[392]
**Creating Auto Response Scripts**[393]
**Account Editor » Autoresponders**[359]

### 6.2.2.2 White List




Use Autoresponder » White List to configure global exceptions to autoresponders. Messages from entries in this list will not receive any autoresponders. Both email addresses and header/value pairs can be included in the list. Enter one address or header/value pair per line. Wildcards are permitted.

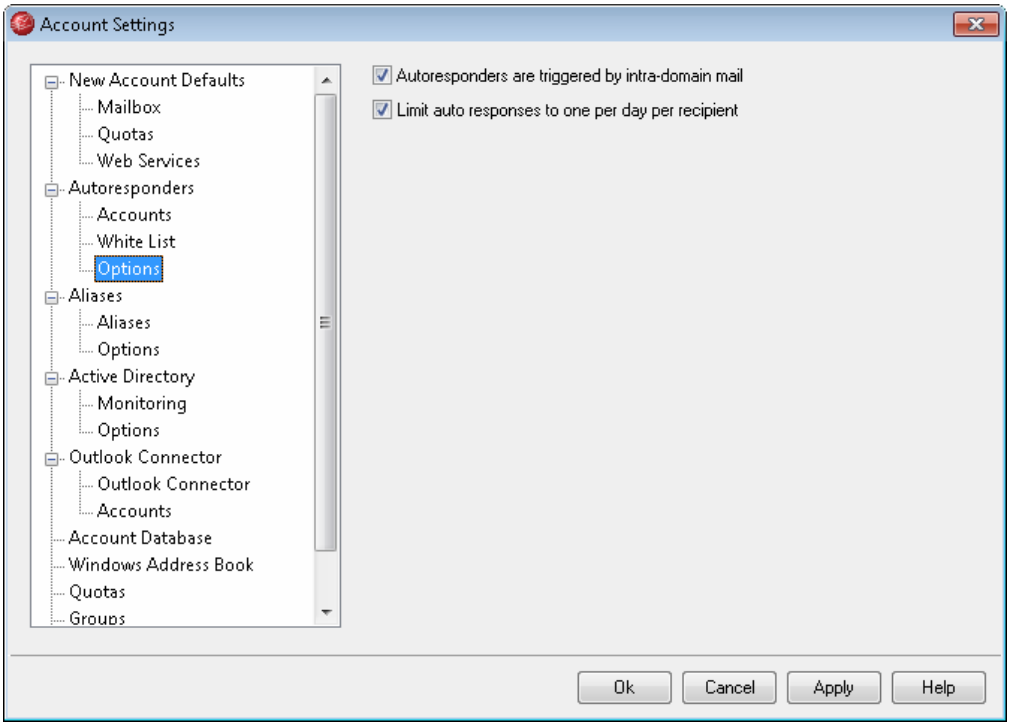
All system addresses (i.e. mdaemon@*, mailer-daemon@*, and so on) should be listed to help prevent mail loops and other problems.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**Autoresponders » Accounts** 390
**Autoresponders » Options** 392
**Creating Auto Response Scripts** 393
**Account Editor » Autoresponders** 359

### 6.2.2.3 Options




**Options**

**Autoresponders are triggered by intra-domain mail**
By default, both local and remote mail will trigger autoresponders. Clear this box if you do not wish mail that is sent from one local MDaemon domain to another to trigger them.

**Limit auto responses to one per day per recipient**
By default, autoresponders will only generate one response message per day for any given address. This prevents people from receiving the same redundant auto response message from you over and over again on the same day, every time they you an email. Clear this box if you wish to send auto response messages each time someone sends you a message, even if they have already received one that day.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

This option also helps to prevent message loops, which can occur when your auto response message is returned to an address that also has an autoresponder active. Instead of allowing both addresses to send auto response messages constantly back and forth to each other, this option would allow only one message to be sent to that address per day.

**See:**

**Autoresponders » Accounts** 390
**Autoresponders » White List** 391
**Creating Auto Response Scripts** 393
**Account Editor » Autoresponders** 359

### 6.2.2.4 Creating Auto Response Scripts

Auto response scripts are text files that define the messages that are returned as the result of an autoresponder. These scripts are constructed as plain ASCII text files ending with the "`*.rsp`" file extension. When an auto response script is triggered by an autoresponder, the script file is processed and scanned for macros, which will then be replaced by actual data from the incoming message that triggered the response. Lines beginning with the "`#`" character are ignored and are used for comments.

There are several samples of scripts listed below, and there are several generic "`*.rsp`" files provided for you in MDaemon's `\app\` folder.

## Auto Response Script Macros

`$HEADERS$` This macro will be replaced by all of the incoming message's headers. Text immediately preceding this macro will be duplicated at the start of each expanded line.

`$HEADER:XX$` This macro will cause the value of the header specified in place of "`xx`" to be expanded in the message. For example: If the incoming message has "`TO: joe@example.com`" then the `$HEADER:TO$` macro will expand to "`joe@example.com`". If the original message has "`SUBJECT: This is the subject`" then the `$HEADER:SUBJECT$` macro would be replaced with the text "`This is the subject`".

`$BODY$` This macro will be replaced by the entire message body. In an attempt to preserve character sets for different languages, MDaemon will read the message body as binary data rather than pure text, thus

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

| | |
|---|---|
| | allowing a byte-for-byte copy of the message body. |
| $BODY-AS-TEXT$ | Like the $BODY$ macro, this macro will be replaced by the entire message body, but as text rather than binary. Text immediately preceding this macro will be duplicated at the start of each expanded line. So, using ">>$BODY-AS-TEXT$" in a script would place each line of the original message into the generated message, but each line would begin with ">>". Text can also be added to the right of this macro. |
| $ATTACHMENTS$ | This macro will be replaced by the entire list of all attached files extracted from the original message. Text immediately preceding this template variable will be duplicated at the start of each expanded line.<br><br>For example: FILE-LIST: $ATTACHMENTS$ would place each attachment file name into the generated message, preceded by the text string, "FILE-LIST: ". |
| $ATTACHMENTCOUNT$ | This macro will be replaced with an integer value equal to the number of attachments extracted from the original message. |
| $ATTACHMENT(X)$ | This macro will be replaced with the attachment file name of the relative attachment number passed in the X parameter. If the value in X is greater than the total number of attached files then the entire variable is removed and replaced with nothing. |
| $SENDER$ | This macro resolves to the full address contained in the incoming message's "From:" header. |
| $SENDERMAILBOX$ | This macro resolves to the mailbox of the sender. The mailbox is the portion of the email address to the left of the "@" symbol. |
| $SENDERDOMAIN$ | This macro resolves to the domain of the sender. This is the portion of the email address to the right of the "@" symbol. |
| $RECIPIENT$ | This macro resolves to the full address of the message recipient. |
| $RECIPIENTMAILBOX$ | This macro resolves to the mailbox of the message recipient. The mailbox is the portion of the email address to the left of the "@" symbol. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| $RECIPIENTDOMAIN$ | This macro resolves to the domain of the message recipient. The domain is the portion of the email address to the right of the "@" symbol. |
| $SUBJECT$ | This macro resolves to the value of the "Subject:" header. |
| $MESSAGEID$ | This macro resolves to the value of the "Message-ID " header. |
| $CONTENTTYPE$ | This macro resolves to the value of the "Content-Type" header. |
| $PARTBOUNDARY$ | This macro resolves to the value of the MIME "Part-Boundary" value found in the "Content-Type" header for multipart messages. |
| $DATESTAMP$ | This macro expands to an RFC-2822 style date-time stamp line. |
| $ACTUALTO$ | Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro expands to that value. |
| $ACTUALFROM$ | Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro expands to that value. |
| $REPLYTO$ | This macro resolves to the value found in the " ReplyTo" header. |
| $PRODUCTID$ | This macro expands to the MDaemon version information string. |

## Header Replacement Macros

The macros listed below control the auto response message's headers.

**%SetSender%**
ex: %SetSender%=mailbox@example.com
Just for the purpose of the auto-response message, this macro resets the sender of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's TO header. For example, if the sender of the original message were "user2@example.org" and recipient's autoresponder used the %SetSender% macro to change it to "user1@example.com" then the auto-response message's TO header would be set to "user1@example.com

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

."

**%SetRecipient%**
ex: `%SetRecipient%=mailbox@example.com`
Just for the purpose of the auto-response message, this macro resets the recipient of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's `FROM` header. For example, if the recipient of the original message were "`michael@example.com`" and Michael's account had an autoresponder using the `%SetRecipient%` macro to change it to "`michael.mason@example.com`," then the auto-response message's `FROM` header would be set to "`michael.mason@example.com`."

**%SetReplyTo%**
`ex: %SetReplyTo%=mailbox@example.com`
Controls the value of the auto-response message's `ReplyTo` header.

**%SetActualTo%**
`ex: %SetActualTo%=mailbox@example.com`
Sets who the "actual" recipient of the message will be.

**%SetSubject%**
`ex: %SetSubject%=Subject Text`
Replaces the value of the original message's subject.

**%SetMessageId%**
`ex: %SetMessageId%=ID String`
Changes the ID string of the message.

**%SetPartBoundary%**
`ex: %SetPartBoundary%=Boundary String`
Changes the part boundary.

**%SetContentType%**
`ex: %SetContentType%=MIME type`
Changes the content-type of the message to the declared value.

**%SetAttachment%**
ex: `%SetAttachment%=filespec`
Forces MDaemon to attach the specified file to the newly generated auto-response message.

#### 6.2.2.4.1 Auto Response Script Samples

A simple auto response script, using several auto response script macros, might be called `VACATION.RSP` and look like this:

```
Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

```
on vacation. Hurray!!!
Yours truly,

$RECIPIENT$
```

You can also use some of the header replacement macros to expand this script and control the headers that will be generated when the auto response message is mailed back to $SENDER$:

```
Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm
on vacation. Hurray!!!
Yours truly,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

Using that script the auto response message will have "RE: " added to the beginning of the subject and have the specified file attached.

The "%SetSubject%=RE: $SUBJECT$" line is handled like this:

1. The $SUBJECT$ portion is expanded and replaced by the original message's subject text. This makes the string equivalent to:

   ```
   %SetSubject%=RE: Original Subject Text
   ```

2. MDaemon replaces the original subject, which it has stored in its internal buffers, with this newly calculated one. From that point forward, any use of "$SUBJECT$" in the script will return the new result.

Note the placement of the new macros - they are listed at the bottom of the response script. This is needed to avoid side effects. For example, if the %SetSubject% macro were placed before the $SUBJECT$ macro, which appears in the second line of the response script, the subject text would have already been changed by the time the $SUBJECT$ macro was expanded. Therefore, instead of replacing $SUBJECT$ with the content of the original message's "Subject:" header, it would be replaced with whatever you have set the value of %SetSubject% to be.

---

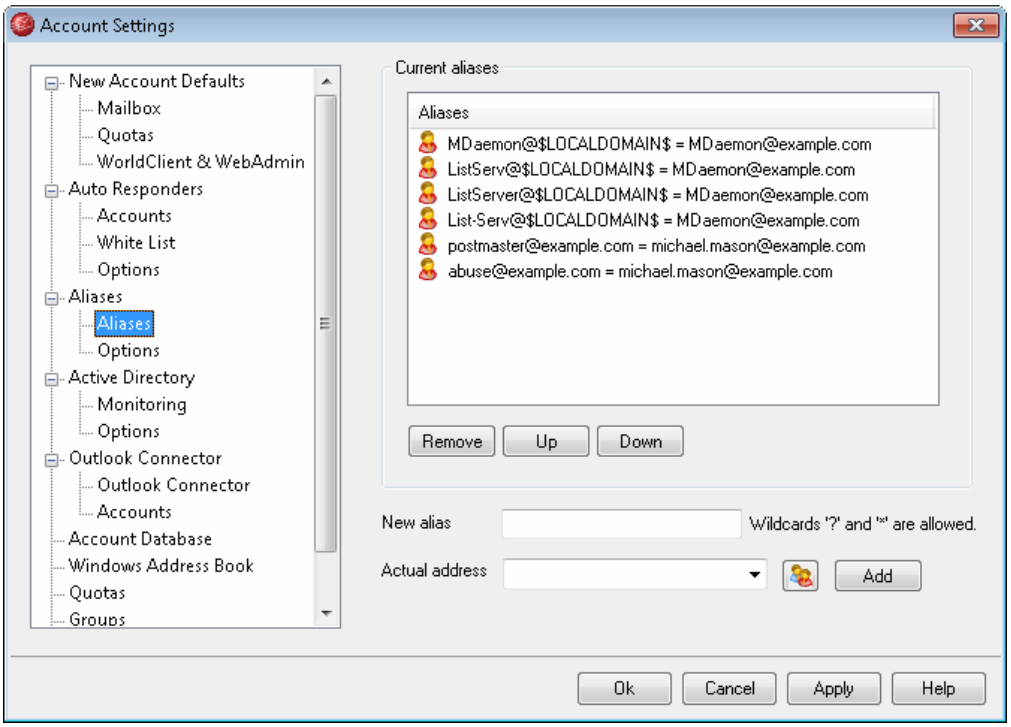
**See:**

**Autoresponders » Accounts** 390
**Autoresponders » White List** 391
**Autoresponders » Options** 392
**Account Editor » Autoresponders** 359

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 6.2.3 Address Aliases

### 6.2.3.1 Aliases




The Aliases options, located at Accounts » Account Settings, make it possible for you to create alternate mailbox names for your accounts or mailing lists, which are useful when you want multiple mailbox names to resolve to a single user account or list. Without aliases you'd have to create separate user accounts for each address and then forward messages or use complicated filter rules to associate them with other accounts.

For example, if `user1@example.com` handled all billing inquiries to your domain, but you wanted to tell everyone to send them to `billing@example.com`, then you could create an Alias so that messages addressed to `billing@example.com` would actually go to `user1@example.com`. Or, if you were hosting multiple domains and wanted all messages addressed to the Postmaster (regardless of the domain) to go to `user1@example.com`, then you could use a wildcard to associate the alias, `Postmaster@*`, with his address.

#### Current Aliases

This window contains all current aliases that you have created.

**Remove**
Click this button to remove a selected entry from the *Current Aliases* list.

**Up**
Aliases are processed in the order in which they are listed. You can move an alias to a higher position in the list by selecting it and then clicking this button.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Down**
Aliases are processed in the order in which they are listed. You can move an alias to a lower position in the list by selecting it and then clicking this button.

—

**New alias**
Enter the email address that you wish to be an alias of the "*Actual address*" listed below. Wildcards of "?" and "*" are acceptable, and you can use "@$LOCALDOMAIN$" in the alias as a wildcard that will match only your local domains. For example: "user1@example.*", "*@$LOCALDOMAIN$", and "user1@$LOCALDOMAIN$" are all valid for use in an alias.

**Actual address**
Select an account from the drop-down list, use the Account icon to browse for an account, or type a new address or mailing list into this space. This is the actual address that will receive the message when it is addressed to a corresponding alias.

**Add**
Click the *Add* button to add the alias to the list. The the *New alias* and *Actual address* values will be combined and placed in the *Current Aliases* window.

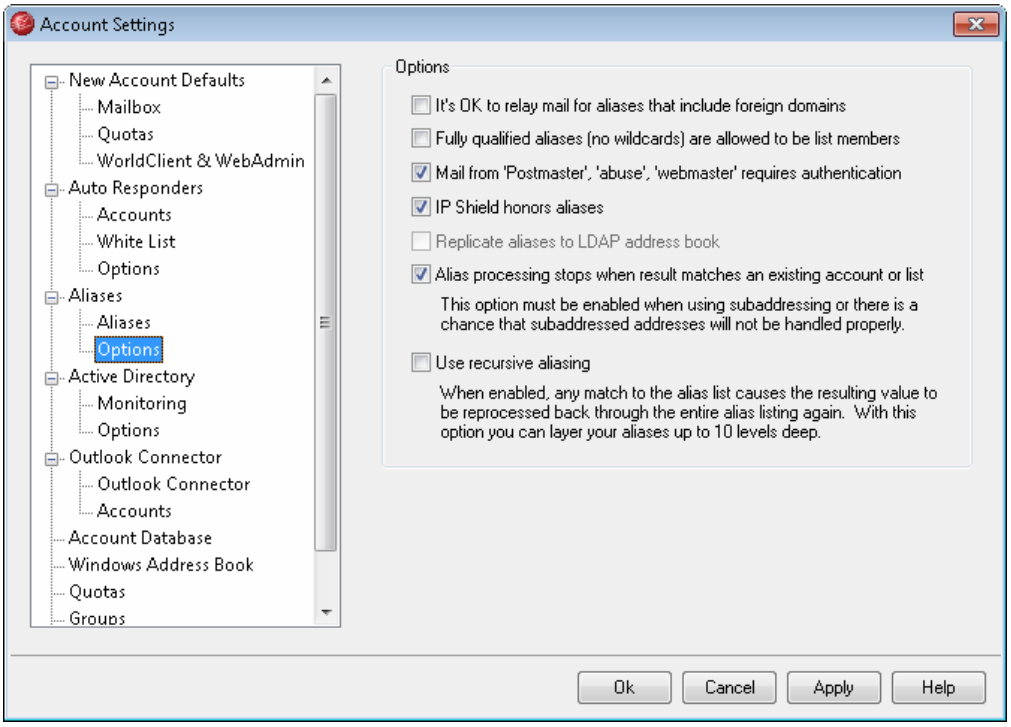
---

**See:**

**Aliases » Options** 400
**Account Editor » Aliases** 368

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.2.3.2 Options




#### Options

**It's OK to relay mail for aliases that include foreign domains**
Check this box if you wish to allow MDaemon to relay mail for aliases that include non-local domains. This option overrides the *Do not allow message relaying* option in Relay Control[271] for those aliases.

**Fully qualified aliases (no wildcards) are allowed to be list members**
Click this checkbox if you want to allow aliases to be members of MDaemon mailing lists. Only actual accounts can be list members if this control is not enabled. **Note:** aliases containing wildcards are not permitted to be list members even if this option is enabled.

**Mail from 'Postmaster,' 'abuse,' 'webmaster' requires authentication**
When this option is enabled, MDaemon will require messages claiming to be from any of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send mail through your system. This option will prevent them and other unauthorized users from being able to do so. For your convenience this option is also available on the SMTP Authentication[280] screen, located at: Security » Security Settings. Changing the setting here will change it there as well.

**IP Shield honors aliases**
By default the IP Shield[273] will honor aliases when checking incoming messages for valid domain/IP pairs. The IP Shield will translate an alias to the true account to

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

which it points and thus honor it if it passes the shield. If you clear this checkbox then the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the IP Shield screen — changing the setting here will be change it there as well.

**Replicate aliases to LDAP address book**
Click this check box if you want aliases to be replicated to the LDAP address book. Alias replication is necessary for the LDAP remote verification feature to work reliably, but if you are not using that feature then replicating aliases to the LDAP address book is unnecessary. If you are not using remote verification then you can safely disable this feature to save processing time. For more information on remote LDAP verification see LDAP 97.

**Aliases processing stops when result matches an existing account or list**
When this option is enabled, alias processing will stop when the recipient of the incoming message matches an existing account or mailing list. This typically applies to aliases that include a wildcard. For example, if you have an alias set to, "`*@example.com=user1@example.com`," then this option will cause that alias to be applied only to addresses that do not actually exist on your server. So, if you also have the account, "`user2@example.com`," then messages addressed to user2 would still be delivered to him because the alias wouldn't be applied to those messages. But messages addressed to some non-existent account or list would be sent to "`user1@example.com`" because the wildcard alias would be applied to those messages. This option is enabled by default.

This option must be enabled when you are using Subaddressing 358, to avoid potential problems with handling those messages.

**Use recursive aliasing**
Click this check box if you want to process aliases recursively. Any alias match causes the resulting value to be reprocessed back through the entire alias list—it is possible to nest aliases up to 10 levels deep. For example, you could set up something like this:

```
user2@example.com = user1@example.com
user1@example.com = user5@example.net
user5@example.net = user9@example.org
```

This is logically identical to the single alias:

```
user2@example.com = user9example.org
```

It also means that:

```
user1@example.com = user9example.org
```

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**Aliases** 398

## 6.2.4 Active Directory

Using the Active Directory options located at Accounts » Account Settings » Active Directory, MDaemon can be configured to monitor Active Directory and automatically create, edit, delete and disable MDaemon accounts when their associated accounts are altered in Active Directory.

### Creating Accounts

When set to monitor Active Directory, MDaemon will query for changes at a designated interval and then create a new MDaemon user account whenever it finds that a new Active Directory account has been added. This new MDaemon user account will be created using the full name, logon, mailbox, description, and enabled/disabled state found within Active Directory.

By default, new MDaemon accounts created as a result of Active Directory monitoring will be added to MDaemon's Default Domain. Alternatively, you can choose to have those accounts added to the domain found within the account's "UserPrincipalName" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain 108 will be created automatically.

### Deleting Accounts

MDaemon can be configured to take one of the following actions when an account is deleted from Active Directory: do nothing, delete the associated MDaemon account, disable the associated MDaemon account, or freeze the associated MDaemon account (i.e. the account can still receive mail but the user can't collect it or access it).

### Updating Accounts

When MDaemon detects changes to Active Directory accounts, it will automatically update the associated properties in the matching MDaemon account.

### Synchronizing MDaemon with Active Directory

A "*Perform full AD scan now*" option is available to cause MDaemon to query the Active Directory database and then create or modify MDaemon user accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it. Then, any future changes made to the Active Directory accounts will be propagated to the MDaemon accounts automatically.

### Dynamic Authentication

Accounts created by MDaemon's Active Directory feature will be setup for Dynamic Authentication by default. With Dynamic Authentication, MDaemon has no need to store the account's password within its own user database. Instead, the account

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

holder will use his or her Windows login/password credentials and MDaemon will pass those to Windows for authentication of the associated account.

To use Dynamic Authentication with Active Directory, a Windows domain name must be present in the space provided on the Monitoring 404. This is the Windows domain that MDaemon will use when attempting to authenticate accounts. In most cases, MDaemon will detect this Windows domain name automatically and fill it in for you. However, you can use an alternate domain in this option if you choose, or you can use "NT_ANY" if you wish to allow authentication across all of your Windows domains instead of limiting it to a specific one. If you leave this option blank then MDaemon will not use Dynamic Authentication when new accounts are created. Instead it will generate a random password, which you will have to edit manually before users will be able to access their mail accounts.

### Persistent Monitoring

Active Directory monitoring will continue to work even when MDaemon is shut down. All Active Directory changes will be tracked and then MDaemon will process them once it restarts.

### Active Directory File Security

It is worth noting that MDaemon's Active Directory features do not alter the Active Directory schema files in any way — all monitoring is one-way from Active Directory to MDaemon. MDaemon will not alter your directory.

### Active Directory Template

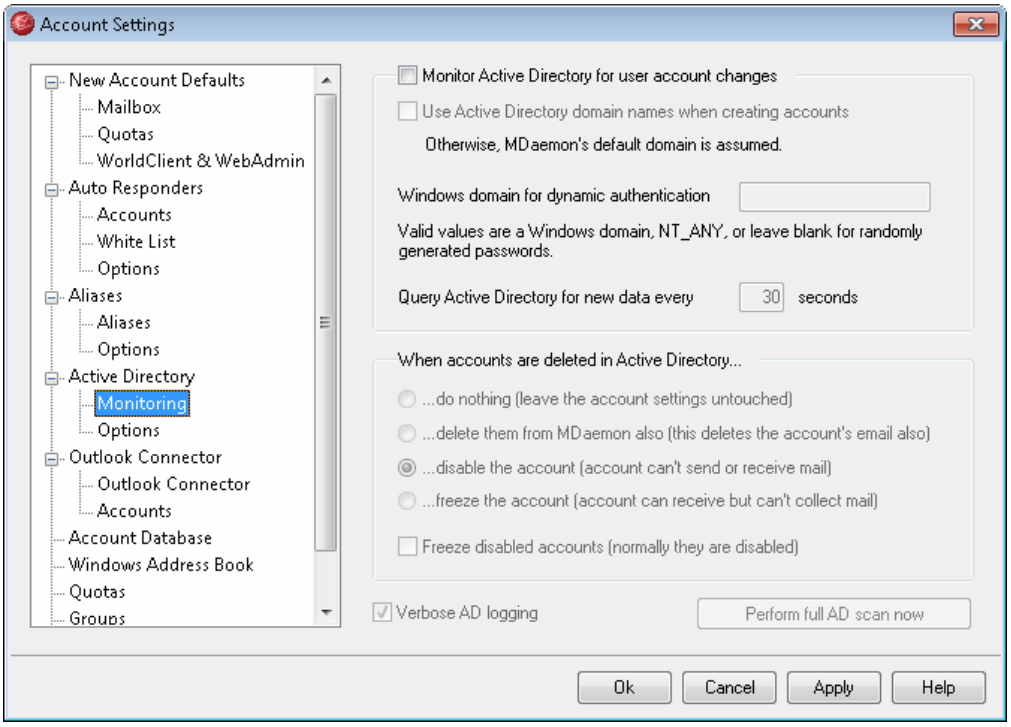
Whenever MDaemon adds or makes changes to accounts due to Active Directory monitoring and scanning, it will use an Active Directory template ("/app/ActiveDS.dat") to link certain Active Directory attribute names to MDaemon's account fields. For example, MDaemon links the Active Directory attribute "cn" to MDaemon's "FullName" field by default. These links, however, are not hard-coded. You can easily edit this template with Notepad if desired and alter any of the default field mappings. For example, "FullName=%givenName% %sn%" could be used as a replacement for the default setting: "FullName=%cn%". See ActiveDS.dat for more information.

**See:**

**Active Directory » Monitoring** 404
**Active Directory » Options** 406

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.2.4.1 Monitoring




#### Active Directory

**Monitor Active Directory for user account changes**
Click this option to activate Active Directory monitoring.

**Use Active Directory domain names when creating accounts**
Use this option if you would like new accounts created as a result of Active Directory monitoring to be added to the domain found within the account's "`UserPrincipalName`" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain[108] will be created automatically. Clear/disable this option if you would like all new accounts to be added to MDaemon's Default Domain.

**Windows domain for dynamic authentication**
Specify a Windows domain name here if you wish to use Dynamic Authentication for accounts created by Active Directory monitoring. If you leave this field blank then new accounts will be assigned random passwords. You will then have to edit those passwords manually in order for the accounts to be accessed.

**Query Active Directory for new data every [XX] seconds**
This is the interval at which MDaemon will monitor Active Directory for changes.

**When accounts are deleted in Active Directory:**
The option selected below determines the action MDaemon will take when an MDaemon account's associated Active Directory account is deleted.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...do nothing**
Choose this option if you do not wish MDaemon to make any changes to an MDaemon account when its associated account is deleted from Active Directory.

**...delete them from MDaemon**
Choosing this option will cause the MDaemon account to be deleted when its associated account is deleted from Active Directory.

This will cause the associated MDaemon account to be completely removed. All of the account's messages, message folders, address books, calendars, and so on will be deleted.

**...disable the account**
When this option is selected and an Active Directory account is deleted, its corresponding MDaemon account will be disabled. This means that the MDaemon account will still exist on the server, but it cannot send or receive email or be accessed by anyone.

**...freeze the account**
When this option is selected MDaemon will still accept the account's incoming mail but effectively "lock" it so that it cannot be accessed. In other words, incoming mail addressed to that account will not be rejected or deleted by MDaemon but the account holder will not be able to collect or access that mail as long is the account is frozen.

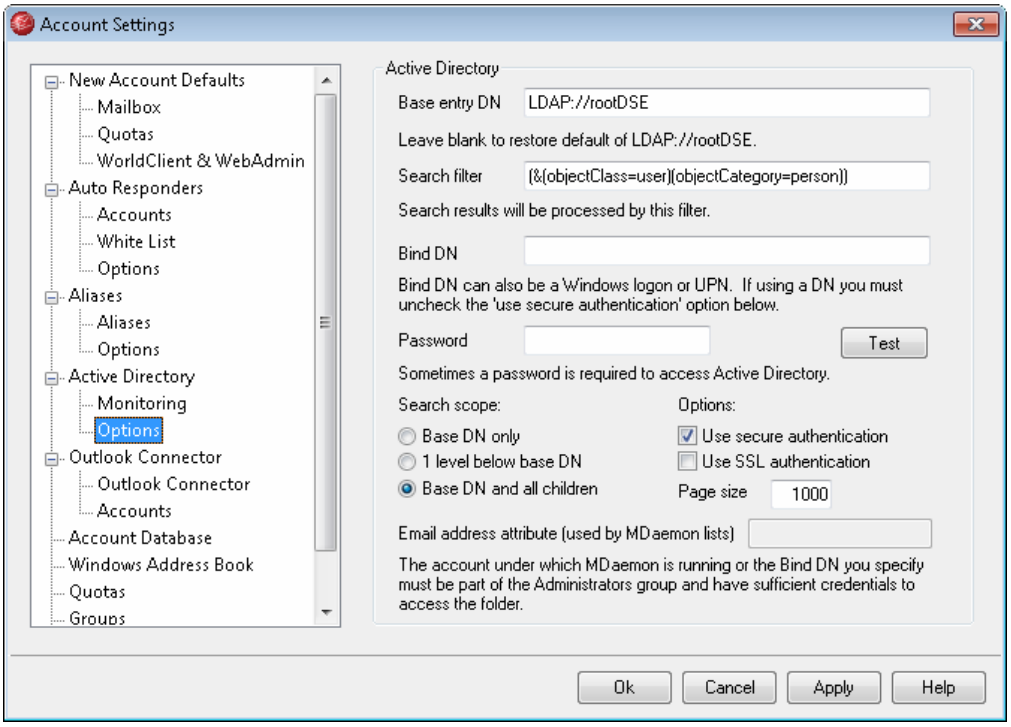
**Freeze disabled accounts**
By default, when you disable an account in Active Directory, MDaemon will also disable the associated account in MDaemon. This makes the account inaccessible and MDaemon will neither accept nor deliver messages for it. However, if you prefer to have the associated MDaemon account frozen instead of disabled, click/enable this option. MDaemon will still accept messages for frozen accounts, but users will not be able to access those accounts to collect or send their email.

**Verbose AD logging**
By default MDaemon will use verbose logging for Active Directory. Clear this checkbox if you wish to use less extensive AD logging.

**Perform full AD scan now**
Click this button to cause MDaemon to query the Active Directory database and then create, edit, or delete accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 6.2.4.2 Options




Access to Active Directory may require special permissions to be set for all features to function.

#### Active Directory Options

**Base entry DN**
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search your Active Directory for accounts and changes. By default MDaemon will begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts in your particular Active Directory tree can reduce the amount of time required to search the DIT for accounts and account changes. Leaving this field blank will restore the default setting of `LDAP://rootDSE`

**Search filter**
This is the LDAP search filter that will be used when monitoring or searching your Active Directory for accounts and account changes. Use this filter to more precisely locate the desired user accounts that you wish to include in Active Directory monitoring.

**Bind DN**
This is the DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

**Password**
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

**Test**
Click this button to test MDaemon's Active Directory configuration.

## Search scope:

This is the scope or extent of your Active Directory searches.

**Base DN only**
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

**1 level below base DN**
Use this option if you wish to extend your Active Directory search to one level below the supplied DN in your DIT.

**Base DN and all children**
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT. This is the default option selected, which when combined with the default Root DSE setting above means that the entire DIT below the Root DSE will be searched.

## Options:

**Use secure authentication**
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

**Use SSL authentication**
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

**Page size**
If the results of an Active Directory query exceed a specified number of entries, then they will be returned in separate "pages" in order to retrieve all the results.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

This setting is the maximum number of entries that will be included per page.

**Email address attribute**

This attribute is used for MDaemon mailing lists and is only available when accessing the Active Directory options located on the Mailing Lists 448 dialog.

## 6.2.5 Outlook Connector for MDaemon

MDaemon PRO supports *Outlook Connector for MDaemon*, a separately licensed product available from Alt-N Technologies. Outlook Connector makes it possible for you to share your Microsoft Outlook calendars, contacts, tasks, and more with other MDaemon users, all without requiring Microsoft Exchange Server. Outlook Connector for MDaemon can effectively eliminate your dependency on Exchange.

When you have installed Outlook Connector for MDaemon, the Outlook Connector screens will be available from MDaemon's menu bar, located at: Accounts » Account Settings » Outlook Connector. This dialog is used for activating and configuring Outlook Connector and for authorizing specific accounts to use it.

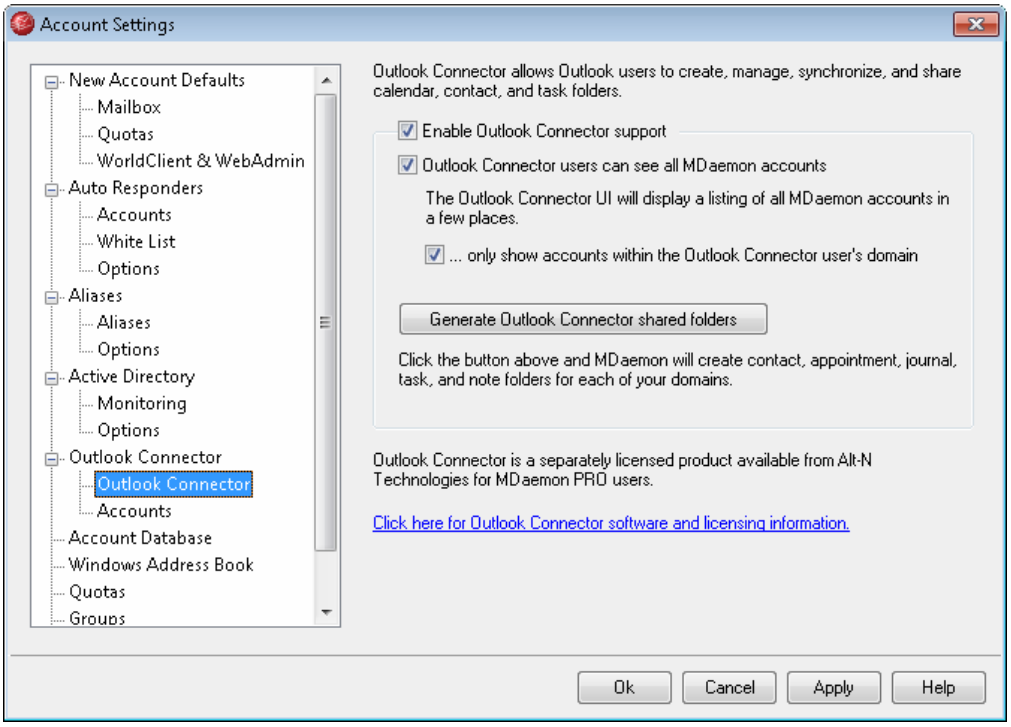
For more information, or to obtain Outlook Connector, visit the Outlook Connector for MDaemon page at www.altn.com.

**See:**

**Outlook Connector Options** 409
**Outlook Connector Accounts** 410

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 6.2.5.1 Outlook Connector Options




#### Outlook Connector

**Enable Outlook Connector support**
Click this checkbox to activate Outlook Connector for MDaemon. Your users will not be able to utilize Outlook Connector's features unless this option is enabled.

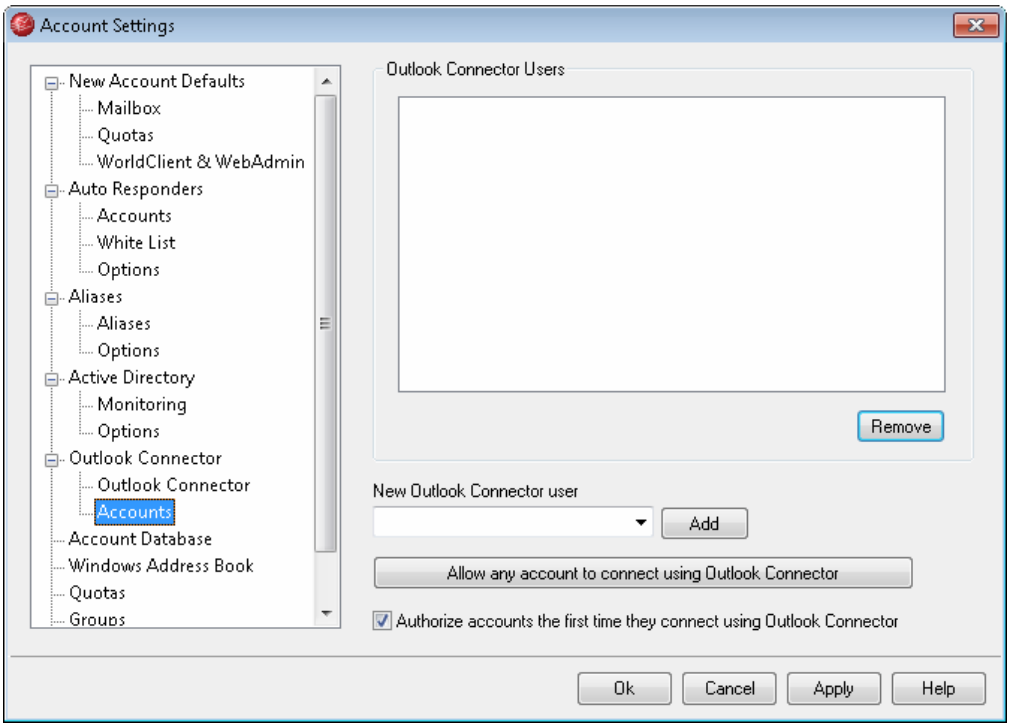
**Outlook Connector users can see all MDaemon accounts**
Click this option if you want all MDaemon accounts that have been authorized to connect via Outlook Connector to be visible on the *Permissions* list that appears in the Outlook Connector for MDaemon Plug-in. Outlook Connector users will choose the accounts from the list whom they wish to grant permission to share their Outlook items. When this feature in disabled, the Outlook Connector Plug-in's *Permissions* list will be blank and the users will have to enter email addresses manually. Only addresses belonging to accounts authorized to connect via Outlook Connector will be able to share the Outlook items. If a user enters an address that is not authorized then the items will simply not be shared with that address unless it is authorized to connect via Outlook Connector at some later time.

**...only show accounts within the Outlook Connector user's domain**
This option is only available when the *Outlook Connector users can see all MDaemon accounts* option above is enabled. Click this checkbox if you want only users who are authorized to connect via Outlook Connector, and who belong to same domain, to appear on the *Permissions* list in the Outlook Connector Plug-in. Accounts belonging to different domains will not be listed even if they are authorized to connect via Outlook Connector.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Generate Outlook Connector shared folders**
Click this button to generate a set of Outlook Connector folders for each domain. It will generate the following folders: Contacts, Appointment, Journal, Tasks, and Notes.

### 6.2.5.2 Accounts




**Outlook Connector Users**

This is the list of MDaemon users who are authorized to share their Outlook folders, Calendars, Contacts, Notes, and so on via Outlook Connector. You can add users to the list by using the options outlined below.

**New Outlook Connector user**
To add an MDaemon user to the list of authorized Outlook Connector users, select the desired user from this drop-down list and then click *Add*.

**Add**
After selecting a user from the *New Outlook Connector user* drop-down list, click this button to add that account to the list of authorized Outlook Connector users.

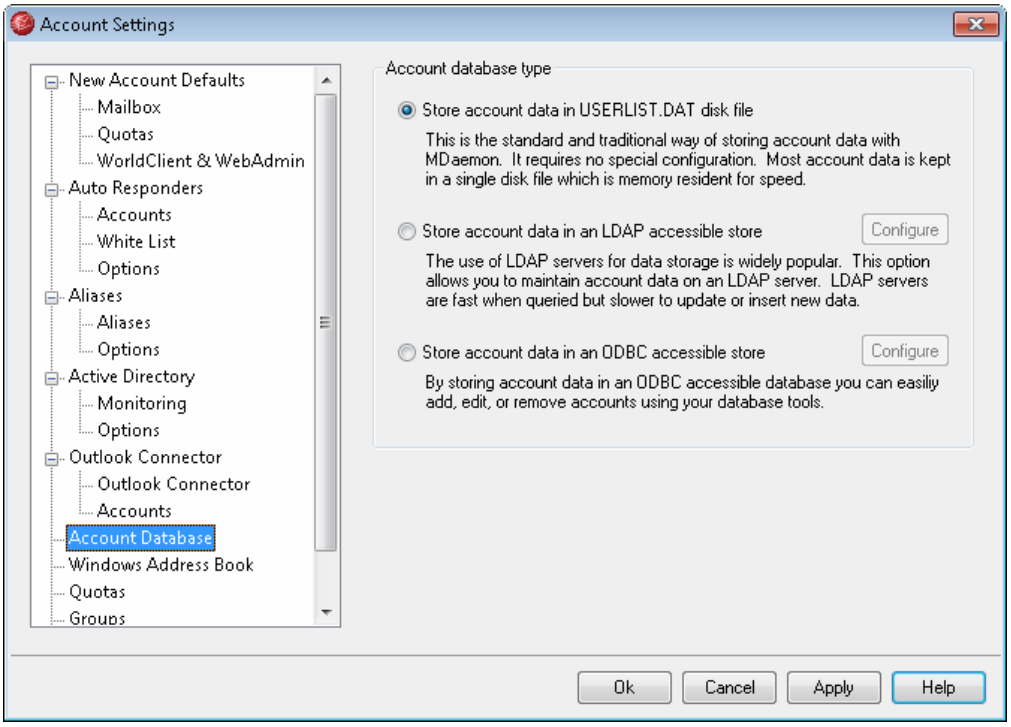
**Remove**
To remove an account from the list of authorized Outlook Connector users, select the desired user in the list and then click *Remove*.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Allow any account to connect using Outlook Connector**
To instantly authorize all MDaemon accounts to connect via Outlook Connector, click this button and all MDaemon accounts will be added to the *Outlook Connector Users* list.

**Authorize accounts the first time they connect using Outlook Connector**
Click this checkbox if you want individual users to be added to the *Outlook Connector Users* list the first time each connects using Outlook Connector. **Note:** if you enable this option then you have in effect authorized all MDaemon accounts to use Outlook Connector for MDaemon. The accounts simply will not be added to the list until the first time each one uses it.

## 6.2.6 Account Database




The Account Database dialog (located under Accounts » Account Settings) is used to designate the method that you want MDaemon to use to maintain your user accounts: ODBC, LDAP, or the local USERLIST.DAT system.

**Store account data in USERLIST.DAT disk file**
Choose this option if you want MDaemon to use its internal USERLIST.DAT file as the account database. This is MDaemon's default setting and causes all of the MDaemon user account information to be stored locally. Most information is stored in a single file, which is memory resident to increase efficiency and speed.

**Store account data in LDAP accessible store**
Choose this option if you want MDaemon to use your LDAP server as the MDaemon

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

user database rather than ODBC or its local USERLIST.DAT system. You might want to use this method of maintaining your user account data if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally. LDAP servers typically respond quickly and efficiently to queries but are slower to update or insert new data.

**Configure**
When the LDAP account data option is selected, click this button to open the LDAP screen 97 for configuring your LDAP server settings.

**Store account data in an ODBC accessible store**
Choose this option if you want to use an ODBC compliant database as your MDaemon account database.

**Configure**
When the ODBC account data option is selected, click this button to open the ODBC Selector Wizard 412 for selecting and configuring your ODBC compliant database.

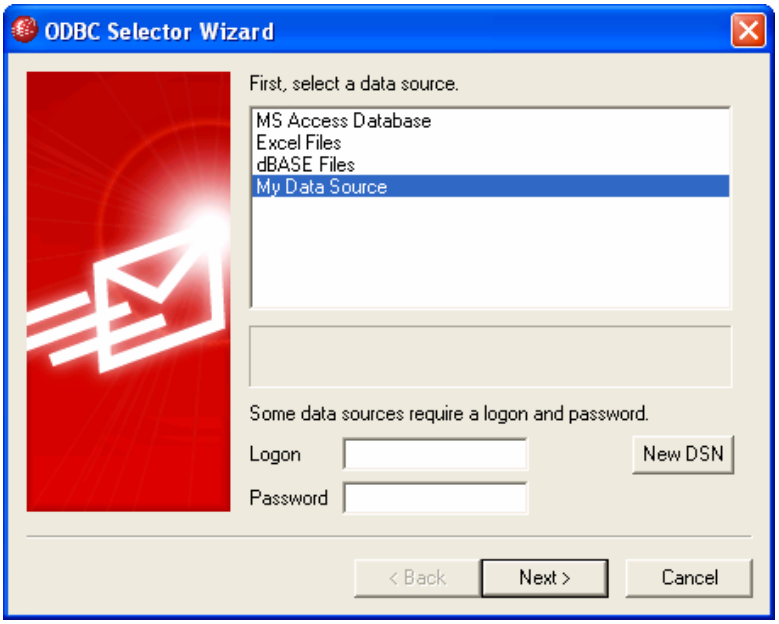
#### 6.2.6.1 ODBC Selector Wizard

Use the ODBC Selector Wizard to select or configure an ODBC compliant data source to use as your MDaemon account database.

## Migrating Your Account Database to an ODBC Accessible Store

1. On the Account Database dialog (Accounts » Account Settings » Account Database), click Store account data in an ODBC accessible store, and then click Configure to open the ODBC Selector Wizard.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

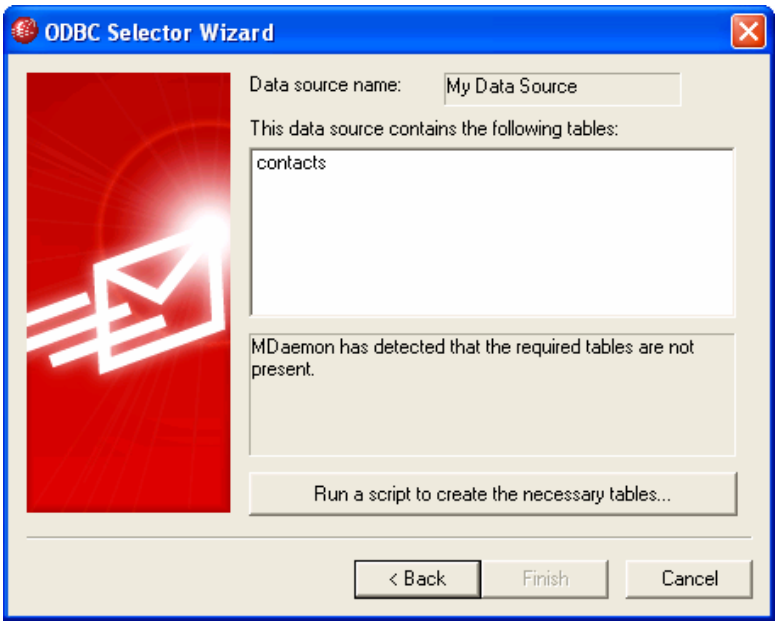



2. Select the data source that you wish to use for your account database. If there is not a compatible data source listed, click New DSN and then follow the instructions listed under, **Creating a New ODBC Data Source** 414.

3. If required, enter the data source's Logon and Password.

4. Click Next.

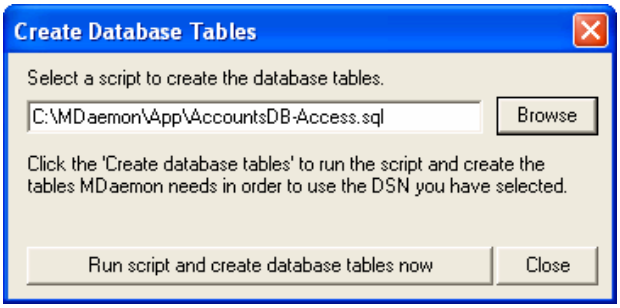
5. If the data source already contains the tables that are required by MDaemon, go to **Step 8**. Otherwise, click Run a script to create the necessary tables...




6. Type the file path (or Browse) to the desired script file that you wish to use to

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

create the tables for your database application. The \MDaemon\app\ folder contains scripts for several of the most popular database applications.




7. Click Run script and create database tables now, Click OK, and click Close.
8. Click Finish, and click OK to close the Account Database dialog.
9. A database migration tool will migrate all of your user accounts to the ODBC data source and then close MDaemon. Click OK, and then restart MDaemon and begin using the new ODBC account database.

**See:**

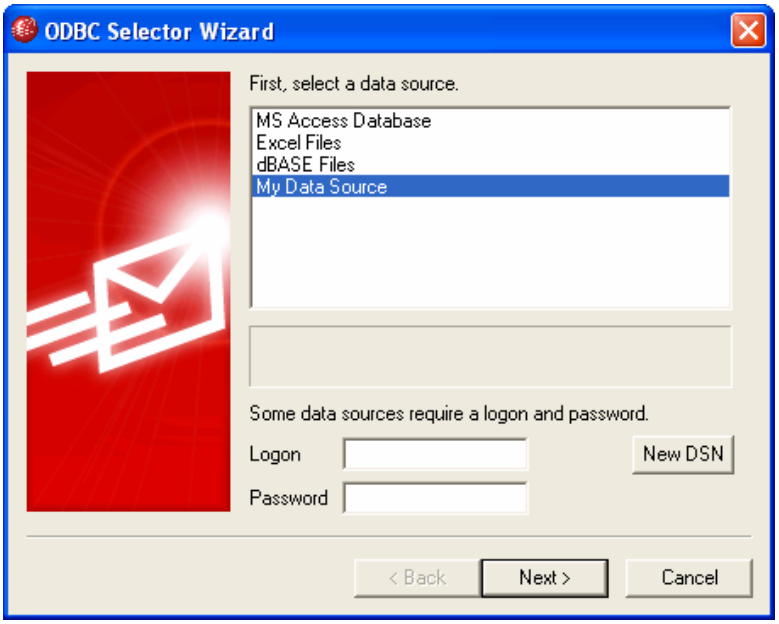
**Account Database** 411
**Creating a New ODBC Data Source** 414

### 6.2.6.1.1 Creating a New Data Source

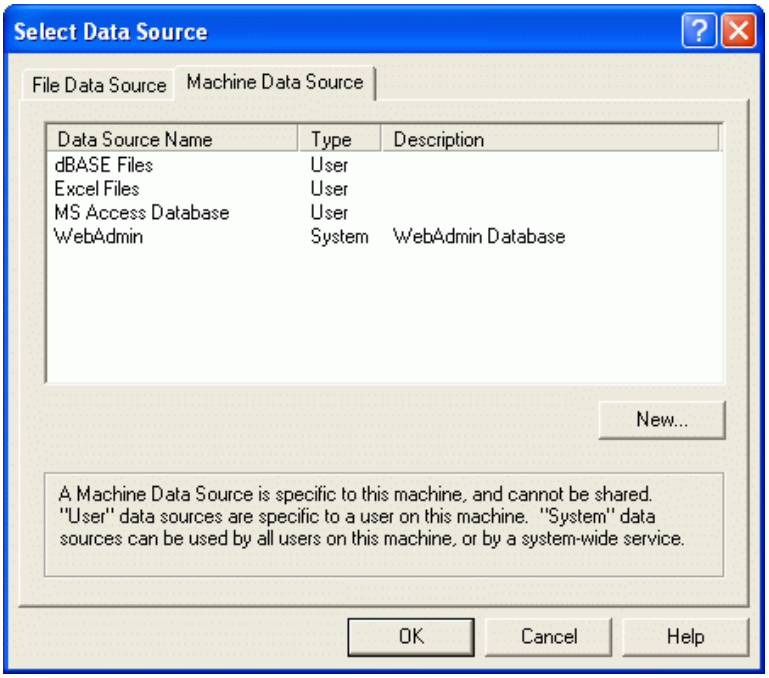
To create a new ODBC data source:

1. On the Account Database dialog (Accounts » Account Settings » Account Database), click Store account data in an ODBC accessible store, and then click Configure to open the ODBC Selector Wizard.
2. Click New DSN to open the Select Data Source dialog.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

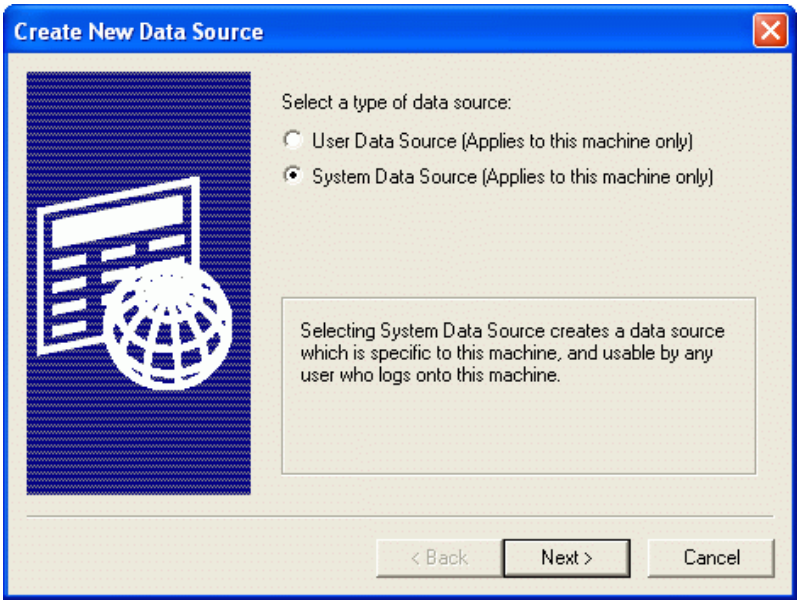



3. Switch to the Machine Data Source tab, and click New... to open the Create New Data Source dialog.

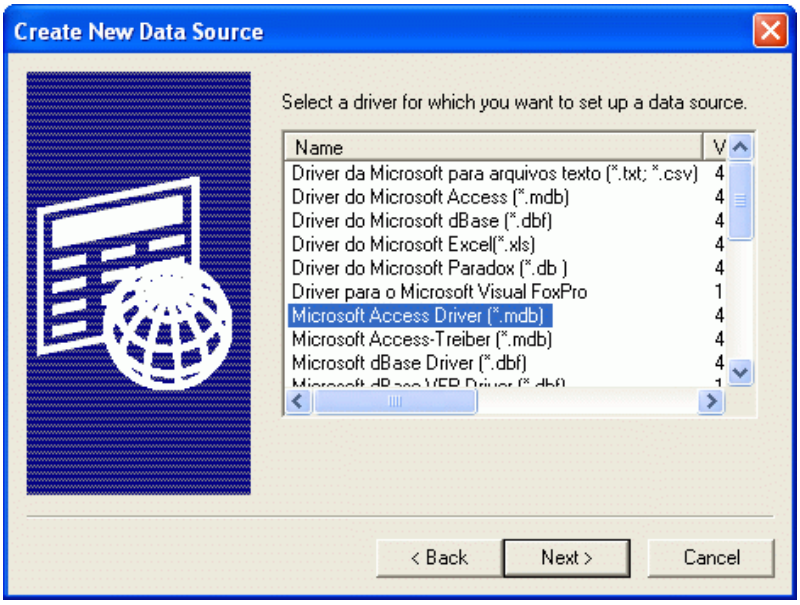



4. Select System Data Source, and click Next.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

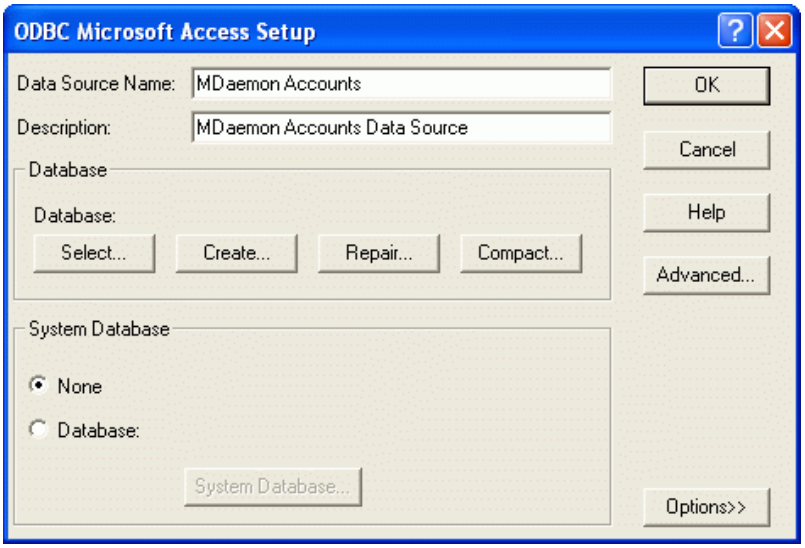



5. Select the database driver for which you wish to set up the data source, and click Next.




6. Click Finish to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.




7. Designate a Data Source Name for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click OK to close the driver-specific dialog.

9. Click OK to close the Select Data Source dialog.

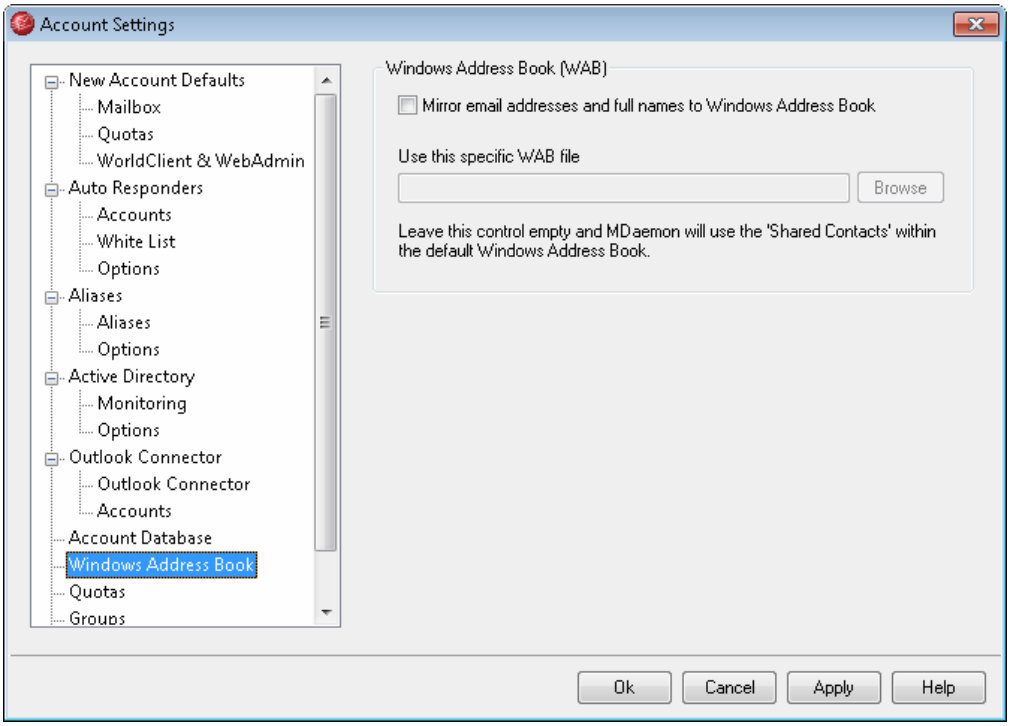
---

**See:**

**Account Database** 411
**ODBC Selector Wizard - Account Database** 412

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 6.2.7 Windows Address Book




MDaemon has the ability to automatically keep a Windows Address Book file (*.wab) or Microsoft Outlook Contact Store current with each account's full name and email address. This is desirable for those who wish to share an address book amongst users of products like Outlook, but do not wish to use an LDAP server or ComAgent for that purpose.

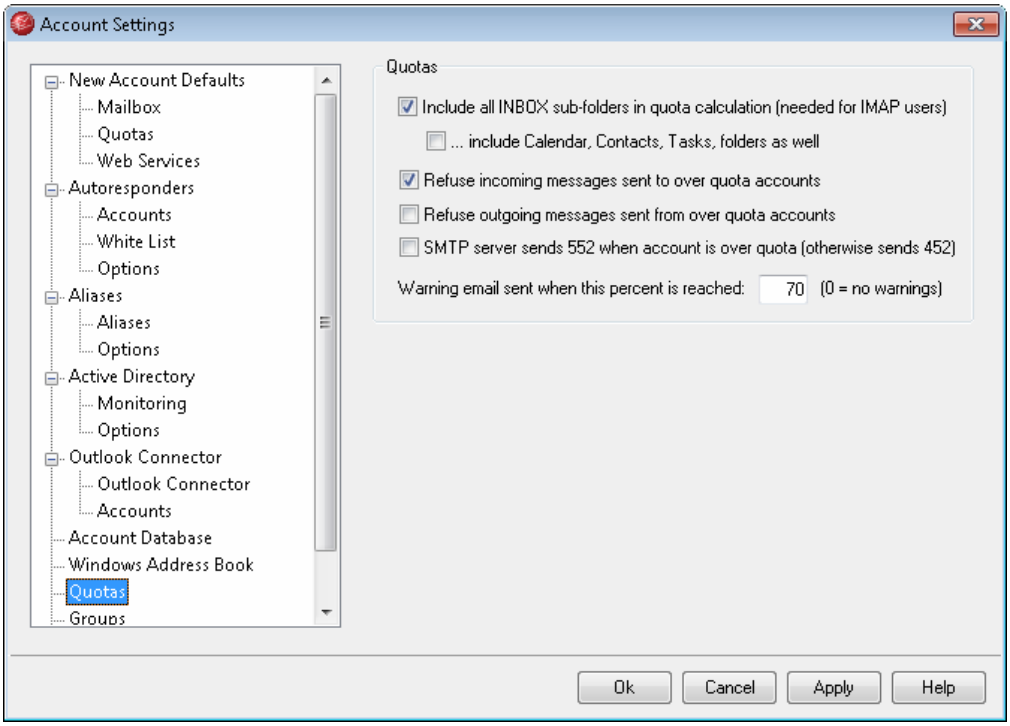
### Windows Address Book (WAB)

**Mirror email addresses and full names to Windows Address Book**
Enable this checkbox if you want your users' names and email addresses to be mirrored to a `*.wab` file or the Microsoft Outlook Contact Store. In the Windows Address Book, on the Tools→Options menu, you can configure whether or not your Windows Address Book will share contact information between Outlook and other applications by storing data in the Microsoft Outlook Contact Store or an address book (`*.wab`) file.

**Use this specific WAB file**
Specify the path to the `*.wab` file in which you wish to mirror your user information. If you leave this control empty then MDaemon will use the shared contacts store within the default Windows Address Book.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## 6.2.8 Quotas




### Quotas

**Include all INBOX sub-folders in quota calculation (needed for IMAP users)**
When this box is checked, all message files in all sub-folders under a user's account will apply toward any size or message number limitations placed on that account. Otherwise, only actual message files in the inbox will count toward those limitations. This is generally only needed for IMAP users.

**...include Calendar, Contacts, Tasks, folders as well**
Click this check box if you wish to include all calendar, contacts, and tasks folders in the quota calculations.

**Refuse incoming messages sent to over quota accounts**
By default, when an account has a message quota restriction placed on it and the quota has been reached, MDaemon will no longer accept any incoming messages for the account until the accountholder deletes some of his or her stored mail. Clear this checkbox if you do not wish to refuse incoming messages for over quota accounts.

**Refuse outgoing messages sent from over quota accounts**
Check this box if you wish to refuse outgoing messages sent from any account that has reached its quota. An over-quota account will no longer be able to send mail until some of its stored messages have been deleted. This option is disabled by default.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

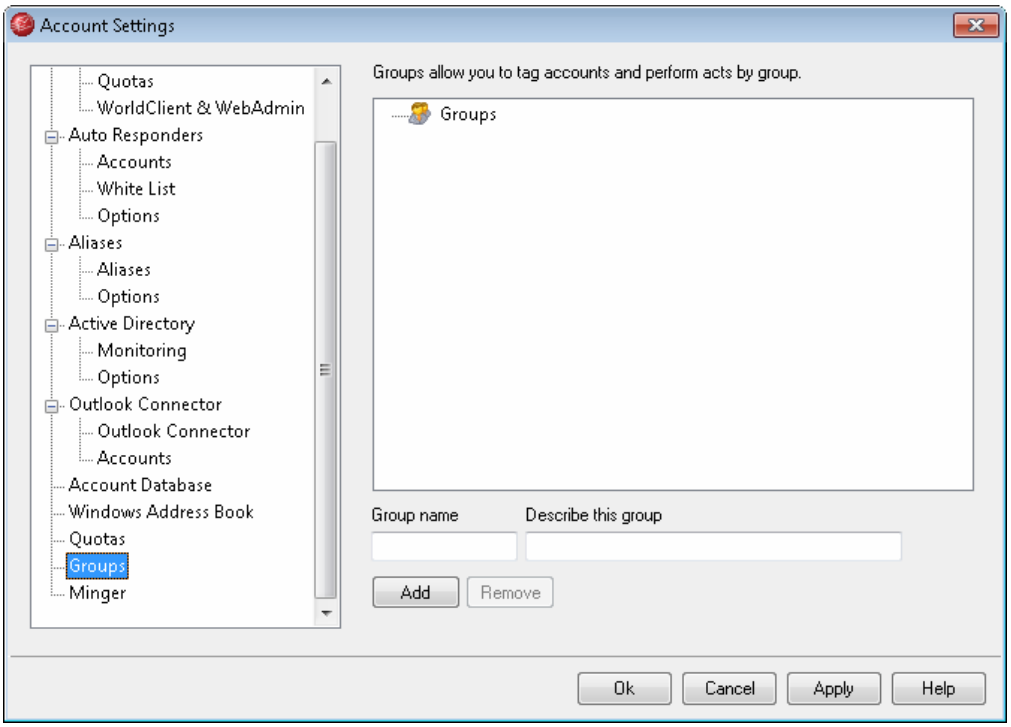
**SMTP server sends 552 when account is over quota (otherwise sends 452)**
By default, when an account is over quota MDaemon sends the 452 error code (i.e "Requested action not taken: insufficient system storage") during the SMTP process. This code generally means that the server should try again later. Check this box if you wish to send the permanent failure 552 error code instead ("Requested mail action aborted: exceeded storage allocation").

**Warning email sent when this percent is reached (0=no warnings)**
When an MDaemon account exceeds this percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* quota restriction designated on the Account Editor 366, a warning message will be sent to the account. This message will list the account's current number of stored messages, the size of its mailbox, and the percentage used and the percentage remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message. Use "0" in this option if you wish to disable warning messages.

**See:**

**Account Editor » Quotas** 366
**New Account Defaults » Quotas** 385

## 6.2.9 Groups




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Groups

Use this dialog to create account Groups to which your user accounts can belong. You can add accounts to a Group by double-clicking the Group in the list. You can also add a user to a Group from the user's account settings 349.

Using the Content Filter, you can create rule conditions 214 based on whether or not the sender or recipient of a message is a member of a specific Group. Further, you can assign Access Control List 79 rights for Shared Folders 74 to specific Groups. Then, all members of that Group will share those access rights.

**Group name**
To create a new group, type its name here, add a short description in the *Describe...* option below, and then click *Add*.

**Describe this group**
Use this text box to add a short description when creating a group.

**Add**
After naming and describing your group, click this button to add it to the Groups list.

**Remove**
To remove a group, select it in the Groups list and then click *Remove*.

### Adding Accounts to a Group

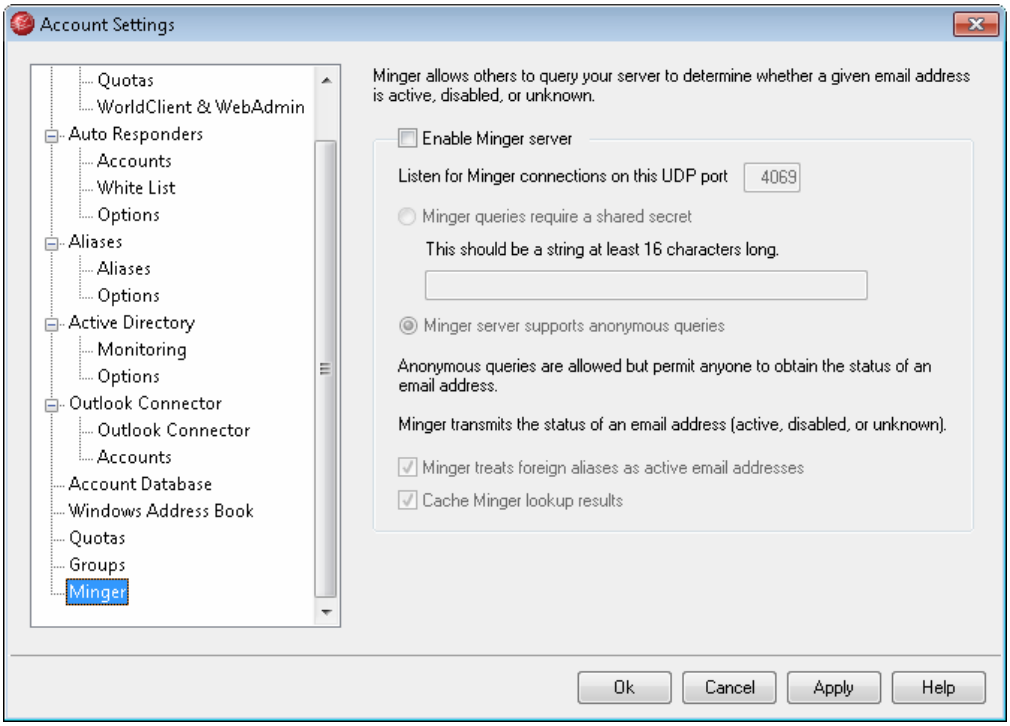
To add accounts to a Group, double-click a Group in the list. You can also add an account to a Group from the Folder, Attachments, Groups 349 screen of the Account Editor.

**See:**

**Folder, Attachments, Groups** 349
**Creating a New Content Filter Rule** 214
**Shared Folders** 74

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## 6.2.10 Minger




Located under Accounts » Account Settings, Minger is an email address verification protocol created by Alt-N Technologies. Originally based loosely on the Finger protocol, Minger is primarily intended to provide a simple and efficient mechanism for allowing others to query your server in order to verify whether or not an email address is valid. For efficiency Minger uses UDP rather than TCP, and for security it can require authentication—though it supports anonymous queries as well. The Minger dialog is used to enable/disable MDaemon's Minger server, designate the port that it will use (the default is 4069), and choose whether to require authentication via a shared secret system or to allow anonymous queries.

MDaemon also has a Minger client, which is built in to the Domain Gateways system (see Verification 461). Each domain for which MDaemon is acting as a gateway or backup server can be configured to use Minger so that MDaemon will connect to the remote server and verify whether or not the recipients of incoming messages for that domain are valid. This prevents you from having to assume that all recipients are valid addresses.

You can find the latest draft of the Minger protocol at:

http://tools.ietf.org/html/draft-hathcock-minger-05

### Minger Server

**Enable Minger server**
Click this checkbox to enable MDaemon's Minger server.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Listen for Minger connections on this UDP port**
This is the port on which the Minger server will listen for connections. The Internet Assigned Numbers Authority (IANA) has reserved and assigned TCP and UDP port 4069 for use with Minger clients and servers. Changing this port is not recommended as it has been reserved exclusively for Minger use.

**Minger queries require a shared secret**
If you wish to require authentication via a shared secret system, choose this option and enter a text string of at least 16 characters. When this option is chosen the Minger server will refuse unauthenticated queries.

**Minger server supports anonymous queries**
Choose this option if you wish to support anonymous Minger queries—the connecting client isn't required to authenticate itself before making address verification queries. This is similar to what can be accomplished now by sources using the `SMTP VRFY` command or SMTP "call back" or "call forward", but it is much more efficient and doesn't result in lots of dropped SMTP sessions over TCP, SMTP logs cluttered with dropped sessions, and similar problems inherent in those methods.

**Minger treats foreign aliases as active email addresses**
When this box is checked, Minger will treat foreign aliases (aliases that point to external addresses) as if they were active known addresses. Also, this behavior is forced when a query comes from SecurityGateway to MDaemon regardless of the state of this option's setting.

**Cache Minger lookup results**
By default MDaemon will cache Minger lookup results. If you do not wish to cache them, disable this option.

## 6.3 Importing Accounts

### 6.3.1 Importing Accounts From a Text File

Click the Accounts→Importing...→Import accounts from a comma delimited text file... menu selection to access this account generation feature. It can also be reached by clicking the *Import* button on the Account Manager. This is a simple method for importing and automatically generating mail accounts. MDaemon will read a text file and generate new mail accounts using as little as just the first and last names of the user. If you are careful to setup your account template strings properly (see New Account Defaults 380) you can generate unique accounts using only the first and last names, but you can also include many other options for specific user settings if you want to override the new account defaults. All fields must be separated by commas.

Each line of the comma delimited text file must contain only a single user's entry. The

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

first line must be a base line giving the names and sequence of the fields in subsequent lines. A sample file would look something like this:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```

The field names in the base line are used by MDaemon to determine the data sequence and can therefore appear in any order. Each of the field names must be in quotes.

All "String" values must be contained in quotes, and a "bool" field value is considered `FALSE` unless the first char is: `y`, `Y`, `1`, `t`, or `T`.

First, middle, and last names are acceptable in each full name. However, you may not use commas in them.

After running the import process, MDaemon will create `TXIMPORT.LOG`, detailing the import results and listing which accounts imported successfully and which failed. Typical reasons why an account might not be imported would include a conflict with an existing account's mailbox, name, or directory information, a conflict with an existing alias to an account, or a conflict with a mailing list name.

See the description of the `MD_ImportUserInfo()` and the `MD_ExportAllUsers()` within the `MD-API.HTML` file located in your `\API\` directory, for more information on the field mappings.

Use the following values in the base line to map to MDaemon account fields:

| Field Name | Type |
|---|---|
| MailBox | string |
| Domain | string |
| FullName | string |
| MailDir | string |
| Password | string |
| AutoDecode | bool |
| IsForwarding | bool |
| AllowAccess | bool |
| AllowChangeViaEmail | bool |
| KeepForwardedMail | bool |
| HideFromEveryone | bool |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| EncryptMail | bool |
| ApplyQuotas | bool |
| EnableMultiPOP | bool |
| MaxMessageCount | int |
| MaxDiskSpace | int |
| FwdAddress | string |
| FwdHost | string |
| FwdSendAs | string |
| FwdPort | string |
| NTAccount | string |
| MailFormat | string |
| AutoRespScript | string |
| AutoRespProcess | string |
| AddToList | string |
| RemoveFromList | string |
| PassMessageToProcess | bool |
| MaxUIDLCount | int |
| MaxMessageSize | int |
| RecurseIMAP | bool |
| MaxInactive | int |
| MaxMessageAge | int |
| MaxDeletedIMAPMessageAge | int |
| Comments | string |
| UserDefined | string |

**See:**

**Windows Account Integration** 425

## 6.3.2 Windows Account Integration

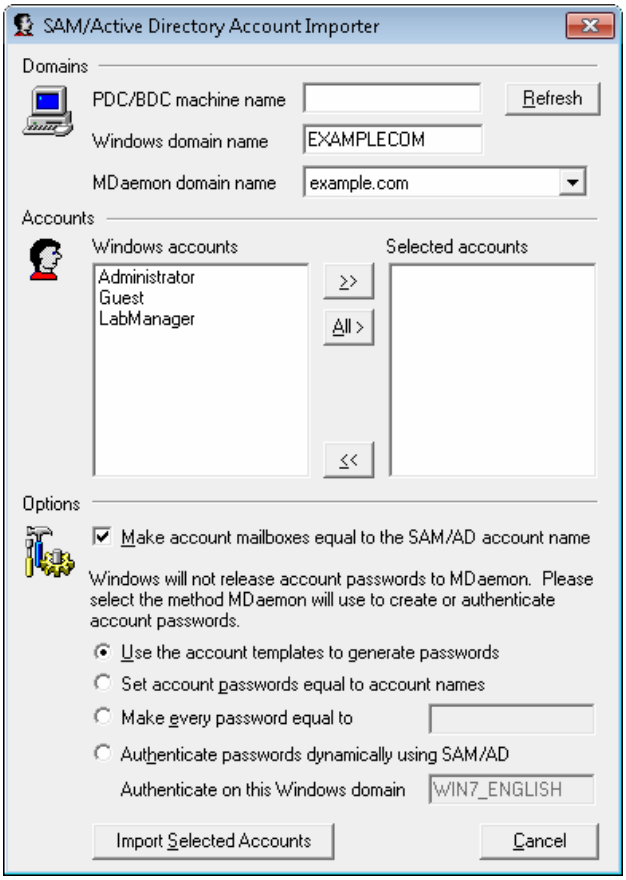
MDaemon supports Windows Account integration. This support consists of a SAM/ Active Directory import engine, which can be reached from MDaemon's Accounts menu (Accounts→Importing...→Import accounts from SAM/Active directory...). Additionally, support for dynamic authentication of users is embedded into the MDaemon user management code. It is possible to specify a Windows domain in an account's password field and then MDaemon will dynamically authenticate such accounts in real-time, using the specified Windows domain's security system. Under such a scheme, changing the account's password in Windows user management will automatically update MDaemon. Therefore, your users will only have to remember one

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

set of authentication credentials. This also makes for very easy account setup for new installations.

The security context of the account running MDaemon must have the **SE_TCB_NAME** privilege (i.e. "To act as part of the Operating System"). If the process is a service running in the *Local System* account, it will have this privilege by default. Otherwise, it must be set in the Windows user manager for the account under which MDaemon is running.

### SAM/Active Directory Account Importer




### Domains

#### PDC/BDC Machine name

This field allows you to specify the machine name from which MDaemon will read Windows account database information. You can specify \\<DEFAULT> and MDaemon will read data from the local machine.

#### Refresh

Click this button to refresh the Windows Accounts listing.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Windows domain name**
Type the Windows domain name from which you wish to import accounts.

**MDaemon domain name**
Choose from the drop-down list box the MDaemon domain into which the accounts will be imported.

## Accounts

**Windows accounts**
This window contains a list of all the account names collected from the Windows account database.

**Selected accounts**
This window contains all the account names that you have selected and wish to import.

**>>**
Click this button to move the highlighted account names from the "Windows Accounts" window into the "Selected Accounts" window.

**<<**
Click this button to remove the highlighted entries from the "Selected Accounts" window.

## Options

**Make account mailboxes equal to the SAM/AD account name**
Click this switch to force each imported user's Windows account name to be used as their Mailbox value. With this method, you will not need to worry about setting up the correct New Account Template 380 macros.

**Use the account template to generate passwords**
This option causes MDaemon to generate passwords for imported accounts using the account template settings (see Account Defaults 380).

**Set account passwords equal to account names**
This switch causes MDaemon to use the account name as the account password.

**Make every password equal to...**
This switch allows you to specify a static password value that will be used by all imported accounts.

**Authenticate passwords dynamically using SAM/AD**
This switch enables dynamic authentication of imported accounts. Rather than specifying a password MDaemon will simply authenticate the mail client supplied USER and PASS values using the NT database in real-time.

**Authenticate on this Windows domain**
Enter the name of the Windows domain that MDaemon will use when authenticating

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

connections dynamically. **This is not the machine name of the domain controller. It is the actual name of the Windows Domain.**

When accounts are configured for dynamic authentication, the name of the Windows domain preceded by two backslash characters is used in the account's PASSWORD field and is stored unencrypted within the USERLIST.DAT file. For example, if an account is configured for dynamic authentication on a Windows domain called ALTN, the account's password field will contain the value \\ALTN. The two backslash characters preceding the domain name signify to MDaemon that the password field actually contains the name of a Windows domain and that MDaemon should attempt to authenticate the USER and PASS values provided by the mail client using that domain's account database. For that reason you must not start a password with two backslash characters unless the account is configured for dynamic authentication as described above. In other words, you can't just have regular passwords that start with two backslashes. Passwords beginning with two backslashes are always assumed to be providing a Windows domain name and not a password.

You may enter the two backslashes and Windows domain name combination into an account's password field on the Account tab 343 of the Account Editor. You need not restrict yourself to using the importer in order to setup accounts for dynamic authentication.

**See:**

**Importing Accounts From a Text File** 423
**Account Editor » Account** 343

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section VII

# 7 Lists Menu

## 7.1 Mailing Lists

Mailing Lists, sometimes called Email Groups or Distribution Lists, allow groups of users to be addressed as if they all shared a common mailbox. Copies of email messages sent to the list are distributed to each of the list's members. Lists may contain members with local and/or remote destination addresses, be public or private, moderated or open, be sent in Digest or normal message format, and more.

### Mailing List Editor

The Mailing List Editor is used to create and maintain Mailing Lists and can be reached from the Lists » New List... or Lists » Edit List... menu selection. It includes the following eleven screens:

**Settings** 431
**Members** 433
**Subscription** 436
**Moderation** 440
**Digest** 441
**Routing** 442
**Notifications** 444
**Support Files** 445
**Public Folder** 447
**Active Directory** 448
**ODBC** 450

### Creating a New Mailing List

When the Lists » New List... menu selection is chosen, the Mailing List Editor will be opened for creating the new list. Naming the list and designating the domain to which it will belong are the only required parameters for creating it. All other options will contain default settings. You can change these settings while creating the list or you can change them later by editing it.

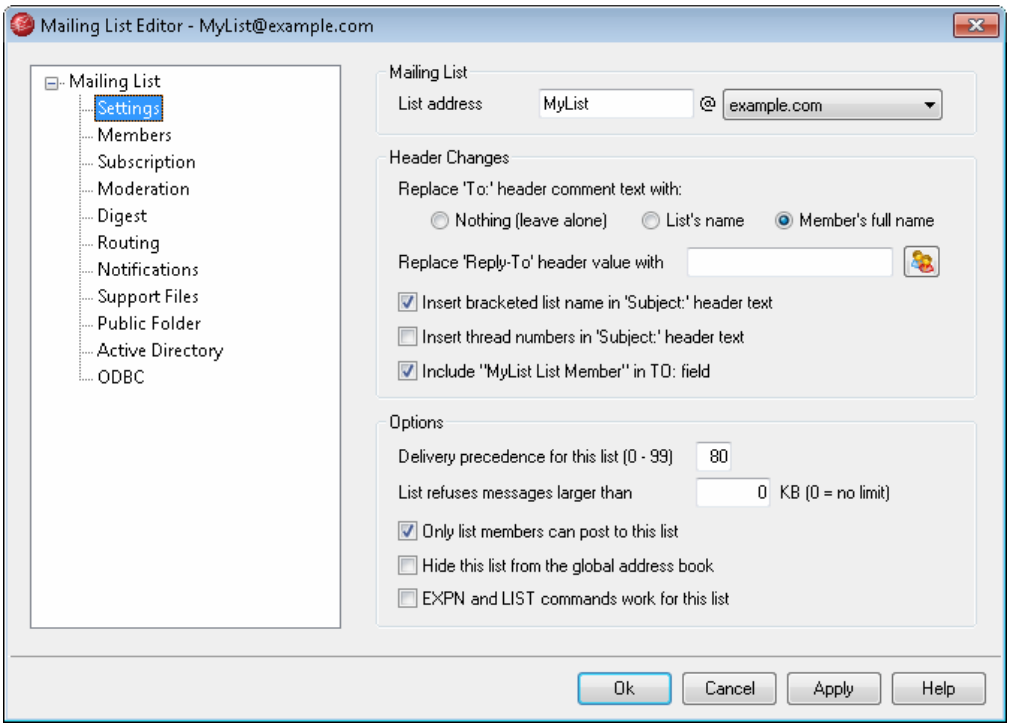
### Modifying an Existing Mailing List

Click the Lists » Edit List... menu selection to open the Select Mailing List dialog. When a list is selected from this dialog it will be opened in the Mailing List Editor for editing or review.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 7.1.1 Mailing List Editor

### 7.1.1.1 Settings




#### Mailing List

**List Address**
Specify a name for the mailing list and then use the drop-down list to choose the domain to which the list will belong. Messages directed to this list will use the name and domain specified here (e.g. `mylist@example.com`). List names cannot contain " ! " or " | ".

#### Header Changes

**Replace 'TO:' header comment text with:**
Use this option to designate the text to display in the comment, or real name, portion of the TO: header whenever MDaemon receives a message directed to the list.

**Nothing (leave alone) -** When this options is selected MDaemon will make no changes to the address displayed. The address contained in the TO: header will appear exactly as the sender of the message entered it.

**list's name -** This option displays the address of the Mailing List in the TO: header.

**member's full name -** When this option is selected, the TO: header will contain the name (if available) and address of the list member to whom the message is directed.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

The *member's full name* option can only be chosen when "*Deliver list mail to each member individually*" has been selected on the Routing screen[442]. When "*Deliver list mail using individual RCPT commands for each member*" is selected, MDaemon will default to the *list's name* option.

**Replace 'Reply-To" header value with**
Type the email address to which you want replies to this list to be directed, or click the Account icon if you wish to browse for a specific account to direct replies to. Use the list's address if you want replies to be directed back to the list. If you leave this field blank then replies to any list message will be directed back to the sender of that message. Traditionally replies to mailing list messages are directed back to the list rather then to the sender of the message that was posted to the list.

**Insert bracketed list name in "Subject:' header text**
This setting causes MDaemon to enclose the name of the list in brackets (e.g. [ListName]) and add it to the beginning of the `Subject:` in all messages sent to the list.

**Insert thread numbers in "Subject:' header text**
This switch allows you to toggle whether thread numbers will be displayed in the `Subject:` header of list messages. They are appended to the end of the subject line in braces and used as a pseudo-thread number. Sorting your inbox by subject will align list mail in chronological order.

**Include 'ListName List Member' in TO: field**
When this feature is enabled, the list's name followed by "List Member" will be displayed in the "real name" portion of the message's TO: field. For example, "`MyList List Member`".

Not all email clients support the displaying of "real names" in the TO: field of messages. In such clients only the actual email address designated in the "*Replace 'TO:' header text with:*" option will appear.

## Options

**Delivery precedence for this list (0-99)**
Enter a number from 0-99 in this control. This value signifies the relative sort order of the messages during the delivery process. The lower the value, the higher its importance and the further up it will be in the sort order within a message queue. As a guideline for assigning values: 10 = Urgent, 50 = Normal, and 80 = Bulk.

**List refuses messages larger than [xx] KB**
This control places an upper limit on the size of a message accepted for this mailing list. Messages larger than this limit are refused.

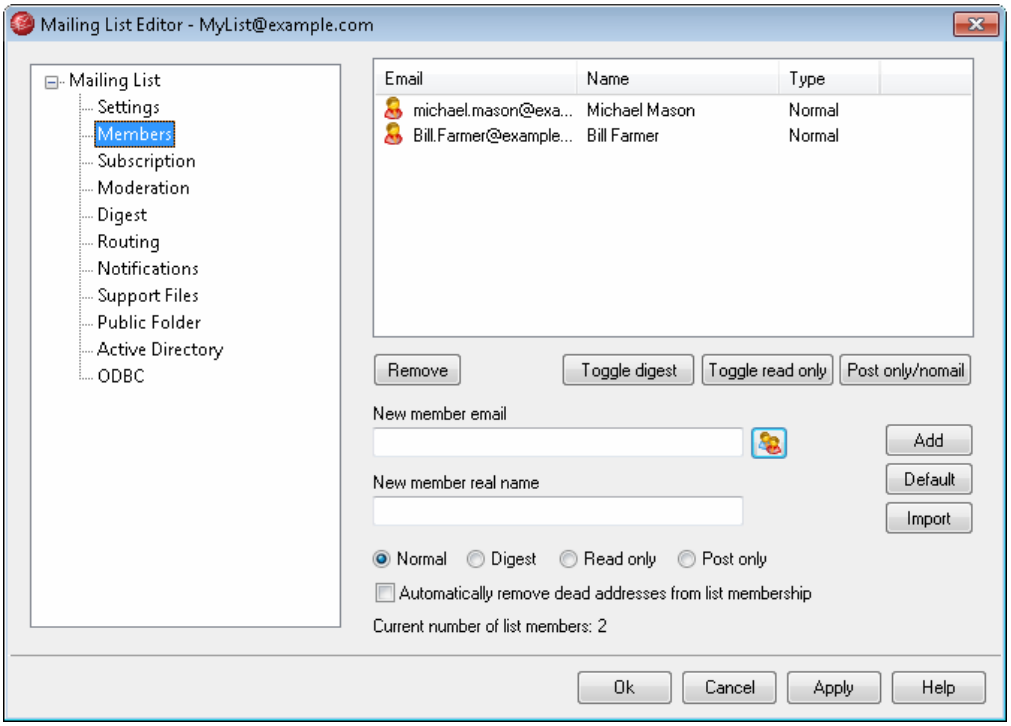
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Only list members can post to this list**
When this control is enabled, the list will be considered a "private" list, meaning that only list members can send messages to the list. Messages originating from non-members will be refused.

**Hide this list from the global address book**
Click this option to hide the mailing list from the WorldClient and LDAP public address books.

**EXPN and LIST commands work for this list**
If this option is selected the membership of the list will be reported in response to an EXPN or LISTS command during a mail session. Otherwise, the list's membership will be kept private.

### 7.1.1.2 Members




**Membership**

This box display the email addresses and names of all members currently subscribed to the list. Each member's entry also states its "type" of membership: normal, digest, read only, or post only.

**Remove**
To remove a member from the list, select its entry and then click this button.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Toggle digest**
Select a member and then click this button to make it a Digest 441 membership.

**Toggle read only**
Select a member's entry and then click this button to switch it to "Read Only" status. The member will still receive messages from the list but will not be allowed to send them to it.

**Post only/no mail**
Clicking this button after selecting a member will set the membership to "Post Only." A Post Only member can send messages to the list but will not receive any.

### Adding New Members

**New member email**
Enter the email address that you wish to add to the mailing list, or click the Account icon if you wish to browse MDaemon accounts to add one to the list. List member addresses cannot contain " ! " or "|".

If you wish to add all of your MDaemon users or all users of one of your domains, then you can enter `ALL_USERS` or `ALL_USERS:<domain>` respectively, instead of entering a specific email address. For example, adding `ALL_USERS:example.com` as a member of a list has the same effect as adding every `example.com` user account separately. Adding `ALL_USERS` as a member is the same as added every MDaemon account, regardless of the domain.

**New member real name**
Enter the member's name in this field. This name will appear in the "To:" header of list messages when the "*Replace 'TO:' header text with: member's full name*" option is selected on the Settings 431.

**Normal, Digest, Read only, Post only**
Click the option that you want to be applied to the *New member's email*.

**Add**
This button adds the entry in the *New member's email* option to the members list.

**Default**
Click any one of the options next to this button (*Normal, Digest, Read Only, Post Only*) and then click the button to make that option the default setting for new members.

**Import**
Click this button to import list members from a text file that has its fields separated by commas (i.e. a comma delimited file). Each entry must be on its own line and all of its fields must be separated by commas. Further, the first line of the file (the baseline) must list the names of the fields and the order in which they appear in the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

remaining lines. One of the fields must be called "**Email**" and contain email addresses. There are also two optional fields: "**FullName**" and "**Type**". FullName is for the list member's name. Type can have a value of: "read only", "post only", "digest", or "normal". All other fields will be ignored by the importer.

For example:

```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St",
"519.555.0100"
```

Imported members do not receive the list welcome packet (if any), and the importer will not check for member duplicates.

**Automatically remove dead addresses from list membership**
When this feature is enabled, MDaemon will automatically remove an address from the members list when it encounters a permanent fatal error while attempting delivery. An addresses is also considered "dead" and removed when the message is moved to the Retry system and subsequently expires from that system.

The *Automatically remove dead addresses...* option is only designed to assist in situations where the remote mail server refuses to accept messages. This will only work when "*Deliver list mail to each member individually*" has been selected on the Routing screen 442. If you are instead routing list messages to a smart host then see *Enhanced List Pruning* below for more information.

**Current number of list members:**
The total number of members currently subscribed to the list is displayed at the bottom of the screen.

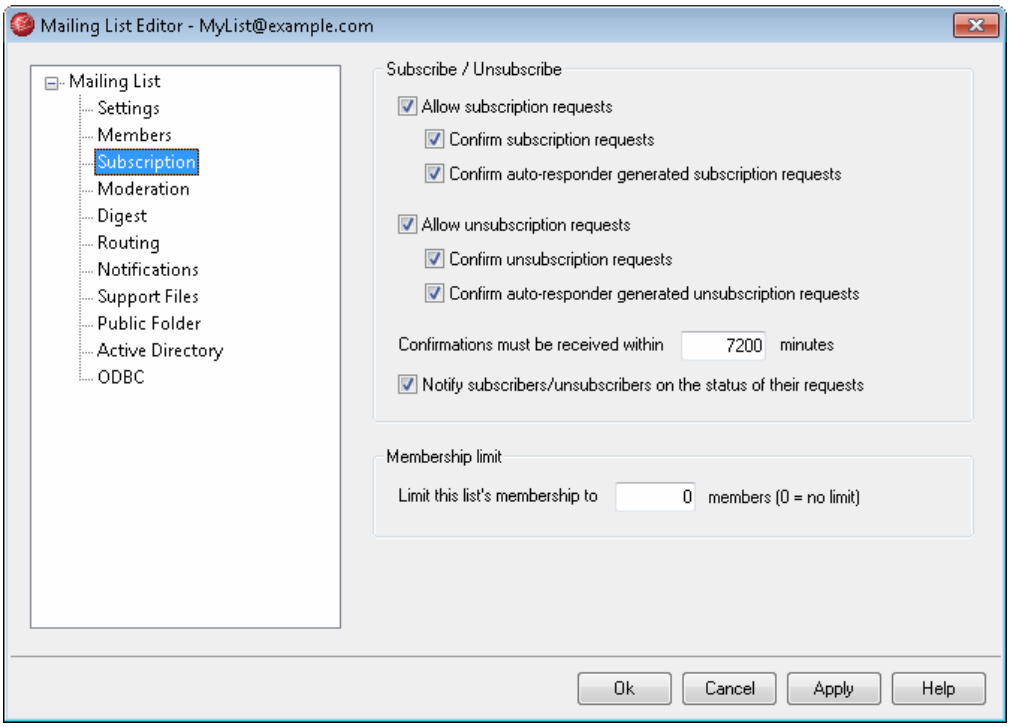
## Enhanced List Pruning

When the *Automatically remove dead addresses...* option is enabled and you have specified a local mailbox as the return path for the list's messages (see the *List's SMTP 'Bounce' address* option on Notifications 444), each day at midnight MDaemon will attempt to parse problem addresses from the returned mail and remove those members that couldn't be reached. This will aid in more efficiently pruning invalid addresses from mailing lists, especially when you are routing the list's messages to a smart host rather than delivering them directly.

On Preferences » Miscellaneous 202 there are two options related to this feature. The *List pruner deletes messages that don't contain parsable addresses* option will cause returned messages that do not contain a parsable address to be deleted, and the *List pruner saves messages which result in list member removal* option will cause all messages that result in a list member being deleted to be saved.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 7.1.1.3 Subscription




#### Subscribe/Unsubscribe

**Allow subscription requests**
This option controls whether or not the list will allow subscription requests, either through specially formatted email messages or through autoresponders. For more information, see: Subscribing to Mailing Lists[438].

**Confirm subscription requests**
When this box is checked, MDaemon will attempt to confirm subscription requests by generating a unique code and then sending it in a message to the address requesting to join the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below.

**Confirm autoresponder generated unsubscription requests**
When this box is checked, MDaemon will attempt to confirm subscription requests that are generating automatically via the Autoresponder[359] option, "*Add sender to this mailing list.*" As with the previous option, MDaemon will

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

generate a unique code and then send it in a message to the address waiting to be added the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

## Unsubscribe

**Allow unsubscription requests**
This option controls whether or not the list will allow unsubscription requests, either through specially formatted email messages or through Autoresponders. For more information, see: Subscribing to Mailing Lists 438.

**Confirm unsubscription requests**
When this box is checked, MDaemon will attempt to confirm requests to remove a member from the list, by generating a unique code and then sending it in a message to the address requesting to unsubscribe from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member from the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below.

**Confirm autoresponder generated unsubscription requests**
When this box is checked, MDaemon will attempt to confirm unsubscription requests that are generating automatically via the Autoresponder 359 option, "*Remove sender from this mailing list*." As with the *Confirm unsubscription requests* option above, MDaemon will generate a unique code and then send it in a message to the address waiting to be removed from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

**Confirmations must be received within [XX] minutes**
This is the number of minutes that the recipient of a subscription or unsubscription confirmation message has before the message will expire. If this time limit is exceeded before MDaemon receives a reply to the message, then the address will not be added or removed from the list. The address would then need to submit a new request to join or leave the list. The default setting of this option is 7200 minutes (i.e. five days).

This is a global value—it applies to all of your mailing lists rather than to the specific list you are editing.

**Notify subscribers/unsubscribers on the status of their requests**
When this checkbox is enabled, MDaemon will send a completion notification message to the user that has been subscribed/unsubscribed to the Mailing List.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Membership Limit

**Limit this list's membership to [xx] members (0=no limit)**
With this feature you can place an upper limit on the number of people who are allowed to subscribe to the Mailing List. Enter a zero into this field if you do not wish to limit list subscriptions.

This limit only applies to addresses subscribed via the email methods outlined in *Subscribing to Mailing Lists*438. This limit does not apply to subscriptions entered manually on the Members433 screen, nor to subscription requests sent via email when the List password440 is included.

**See:**

**Subscribing to Mailing Lists**438
**Autoresponder**359

## 7.1.1.3.1 Subscribing to Mailing Lists

# Subscribing/Unsubscribing via Email Commands

To subscribe to or unsubscribe from a mailing list, send an email message addressed to `MDaemon` (or any alias thereof) at the domain hosting the mailing list, and place the `Subscribe` or `Unsubscribe` command as the first line of the message body. For example, there is a mailing list called `MD-Support` being hosted by `altn.com`. You can subscribe to the list by composing a message addressed to "`mdaemon@altn.com`" and placing the value: `SUBSCRIBE MD-Support@altn.com` as the first line of the message body. The message subject is irrelevant and can be left blank.

For complete details on how to form this and other control messages, see: Remote Server Control Via Email504.

Occasionally, users will attempt to subscribe/unsubscribe to lists via email by sending the commands to the list itself rather than to the MDaemon system account. This results in the command being posted to the list rather than the user being subscribed or unsubscribed. To help prevent these sorts of messages from being posted to mailing lists, there is an option located at Setup » Preferences » System195, called "*Screen incoming mailing list mail for obvious non-list content.*" This option is enabled by default.

# Subscribing/Unsubscribing via Email Addresses

The option, "*Honor '<List>-subscribe' and '<List>-unsubscribe' addresses,*" located at

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Setup » Preferences » Miscellaneous 202, makes it possible for users to join or quit mailing lists by sending a message to a special email address rather than requiring them to use the email commands described in *Subscribing/Unsubscribing via Email Commands* above. To use this method to join or quit a list, a user would simply send a message to the list's address, but with "-subscribe" or "-unsubscribe" appended to the mailbox portion of the address. For example, if the list's name is, "franks-list@example.com," then a user could subscribe to the list by sending a message to, "franks-list-subscribe@example.com." To unsubscribe from the list, the message would be sent to, "franks-list-unsubscribe@example.com." In both cases the content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

## Subscribing/Unsubscribing via Autoresponders

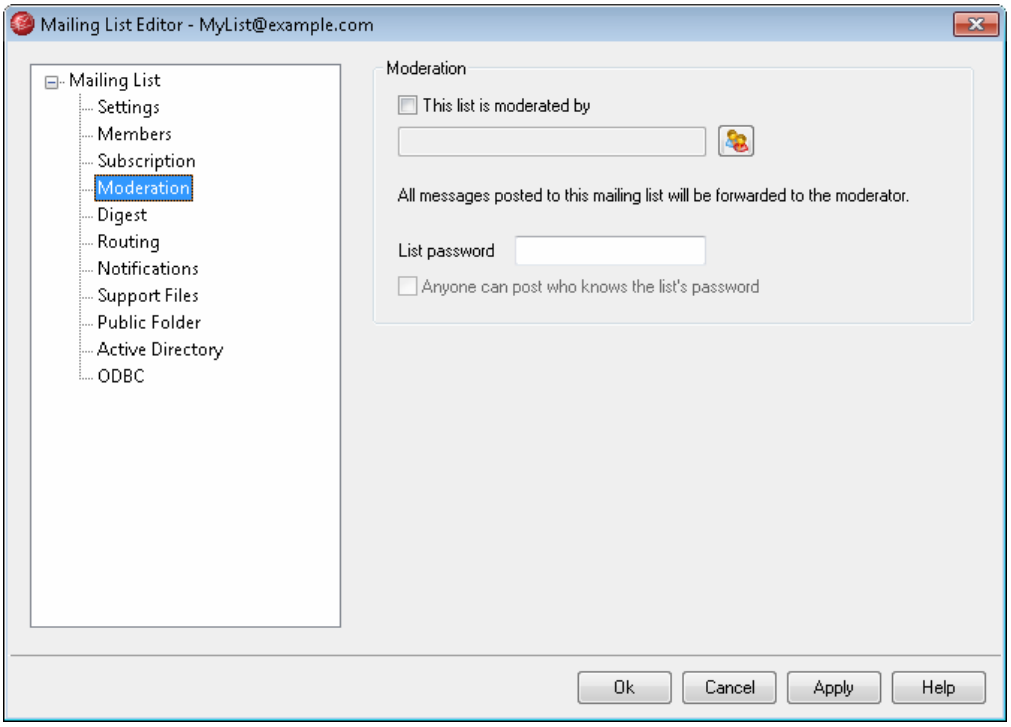
You can also utilize Autoresponders 359 to automatically add or remove list members. To do this you would create one or more MDaemon accounts whose sole purpose would typically be to automatically add or remove addresses who send messages to those accounts, via the Autoresponders configured for each account. For example, if you had a mailing list called, "franks-list@example.com," then you could create an MDaemon account with the address: "join-franks-list@example.com." You would then configure an autoresponder for that account to add to "franks-list@example.com" any addresses sending messages to it. Then, to join that list, all someone would have to do is send an email to "join-franks-list@example.com". This is a simple solution for users because it doesn't require them to remember any of the special email commands required by the *Subscribing/Unsubscribing via Email Commands* method outlined above.

**See:**

**Subscription** 436
**Remote Server Control via Email** 504
**Autoresponder** 359
**Preferences » System** 195
**Preferences » Miscellaneous** 202

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 7.1.1.4 Moderation




#### Moderation

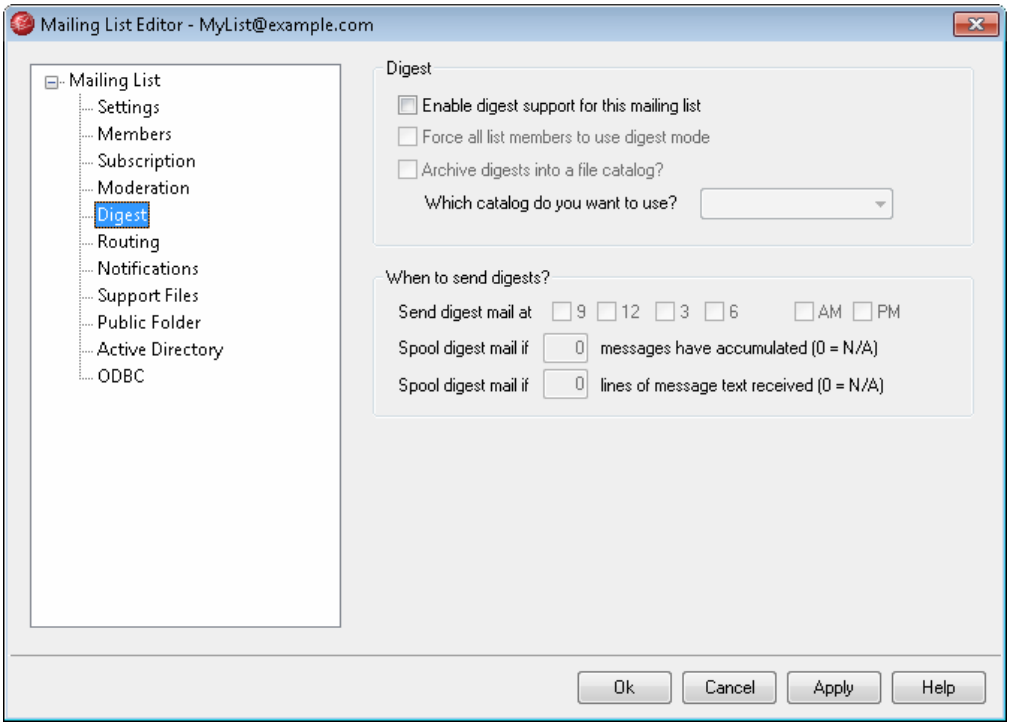
**This list is moderated by**
Check this box and specify an account if you with the list to be moderated by the designated user. Moderated lists forward all posts to the moderator. The moderator alone may submit or forward messages to the list.

**List password**
If you wish to assign a password to this list, then enter it here. List passwords can be used with the *Anyone can post who knows the list's password* option below, and to override the *Membership Limit* option located on the Subscription screen436. They also provide access to a number of features outlined in the *Remote Server Control via Email*504 section.

**Anyone can post who knows the list's password**
If a password is assigned to the list, and this option is enabled, then anyone who includes the list's password at the beginning of a message's subject can post to the list, even if the list is moderated but the sender isn't the moderator.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 7.1.1.5 Digest




#### Digest

**Enable digest support for this mailing list**
Check this box if you wish to allow digest support for this mailing list. When digest support is enabled, a copy of each message sent to the mailing list will be archived so that list members who have their membership type[433] set to *Digest* will periodically be sent batches of these archived messages in a compact and indexed format rather than receive them one at a time.

**Force all list members to use digest mode**
By default, list members can control whether they wish to receive list traffic in digest or normal format. Check this box if you wish to force all members to use digest mode, regardless of the mode they may have chosen for themselves.

**Archive digests into a file catalog / which catalog do you want to use?**
These options allow you to place digest messages into a file catalog so that back-issues of the digests can be collected in the future. MDaemon will generate a unique archive name for each digest and place it into the catalog you specify.

For complete information on how to work with catalogs see: Catalog Editor[478].

#### When to send digests?

The following options determine how often and under what circumstances digests will be sent to those list members who are set to receive mail in digest format. All of the options operate independently of each other, meaning that any or all of them can cause a digest to be sent.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Send digest mail at 9, 12, 3, 6 AM and/or PM**
Use this option to schedule how often this list's digests will be sent. If you check all of the boxes in this option then digests will be sent every three hours, in addition to any that may be triggered by the options below.

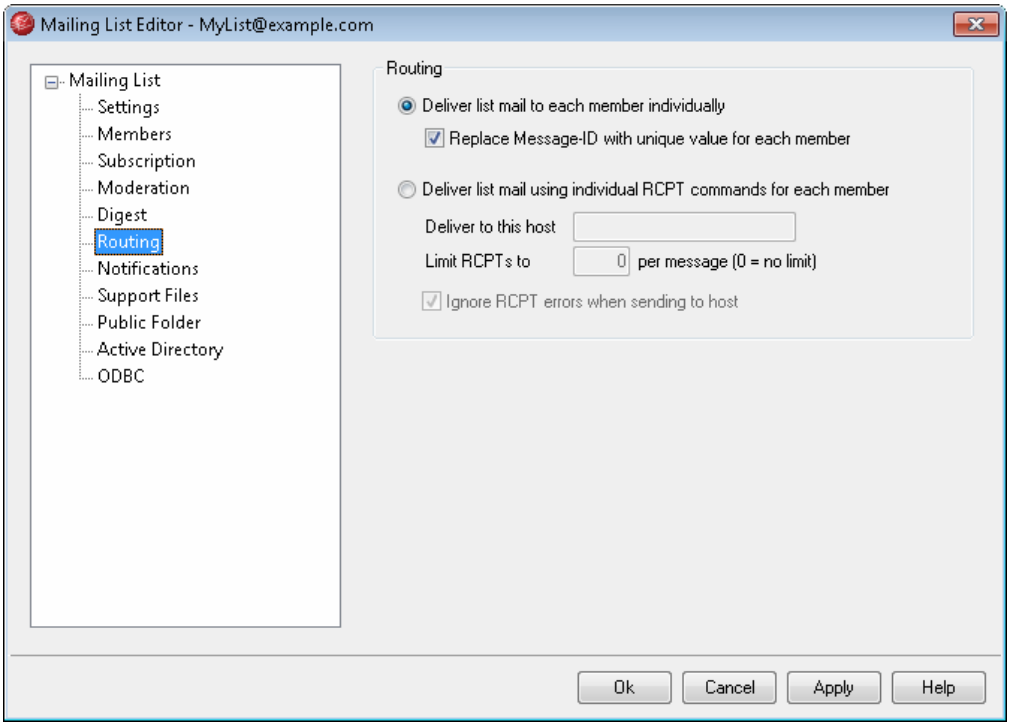
**Spool digest mail if [xx] messages have accumulated (0 = n/a)**
If you wish to send digests automatically whenever a certain number of messages have accumulated, specify that number here. Use "0" if you do not wish to use this option. "0" is the default setting.

**Spool digest mail if [xx] lines of message text received(0 = n/a)**
Entering a value in this option will cause digests to be sent immediately whenever a digest grows to the number of lines of text specified. Use "0" if you do not wish to use this option. "0" is the default setting.

**See:**

**Members** 433
**Catalog Editor** 478
**Remote Server Control via Email** 504

### 7.1.1.6 Routing




Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Routing

**Deliver list mail to each member individually**
If selected, when messages are received for distribution to the list, a separate copy of each message will be created and dispatched to each list member. This will result in numerous individual messages being created which could affect the server's performance, depending on the size of the list and the load on the server.

**Replace Message-ID with unique value for each member**
When MDaemon is set to generate a separate copy of each message for each member, click this checkbox if wish each of those messages to have a unique Message-ID.

**Deliver list mail using individual RCPT commands for each member**
If selected, MDaemon will route a single copy of each list message to the specified smart host, rather then send individual messages to each member. This method employs multiple `RCPT To` statements during the SMTP session with the specified host.

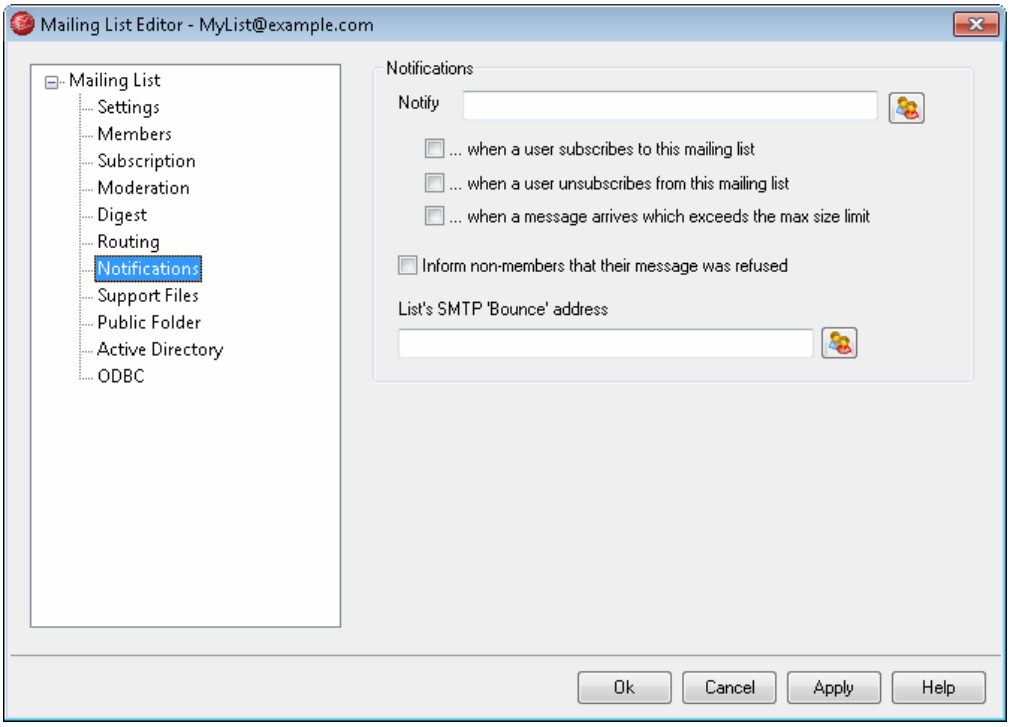
**Deliver to this host**
Designate the smart host to which you wish to pass all of the list's messages for delivery, using RCPT To statements for each member.

**Limit RCPTs to [xx] per message (0=no limit)**
Some hosts limit the number of `RCPT To` statements that they will accept when you are attempting to route a single copy of a message through them. If you specify the limit in this control then MDaemon will work around it by creating additional copies of the message and dividing the list into smaller groups. Then it will deliver the message to those groups thus avoiding the need to exceed the limitation. This is similar to the *Deliver list mail to each member individually* option above, but it generates less copies, sending each copy to groups of addresses rather than generating a separate copy for each member.

**Ignore RCPT errors when sending to host**
Since some smart hosts will refuse to queue or spool mail for certain domains, the routed approach to list delivery could cause numerous problems. An error code returned from the smart host as a result of this refusal would ordinarily cause MDaemon to abort the delivery attempt. Check this option if you want MDaemon to ignore error codes returned from the smart host during delivery of routed list mail, thus allowing those members that are accepted a chance to receive the message.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 7.1.1.7 Notifications




#### Notifications

**Notify**
Use this option to list an address that will be notified when the selected events take place.

**...when a user subscribes to this mailing list**
Check this box if you wish to send a note to the designated address each time someone subscribes to the mailing list.

**...when a user unsubscribes from this mailing list**
Check this box if you wish to send a note to the designated address each time someone unsubscribes from the mailing list.

**...when a message arrives which exceeds the max size limit**
Check this box if you wish to send a note to the designated address each time someone sends a message to the mailing list that is larger than *List refuses messages larger than [xx] KB* limit designated on Settings 431.

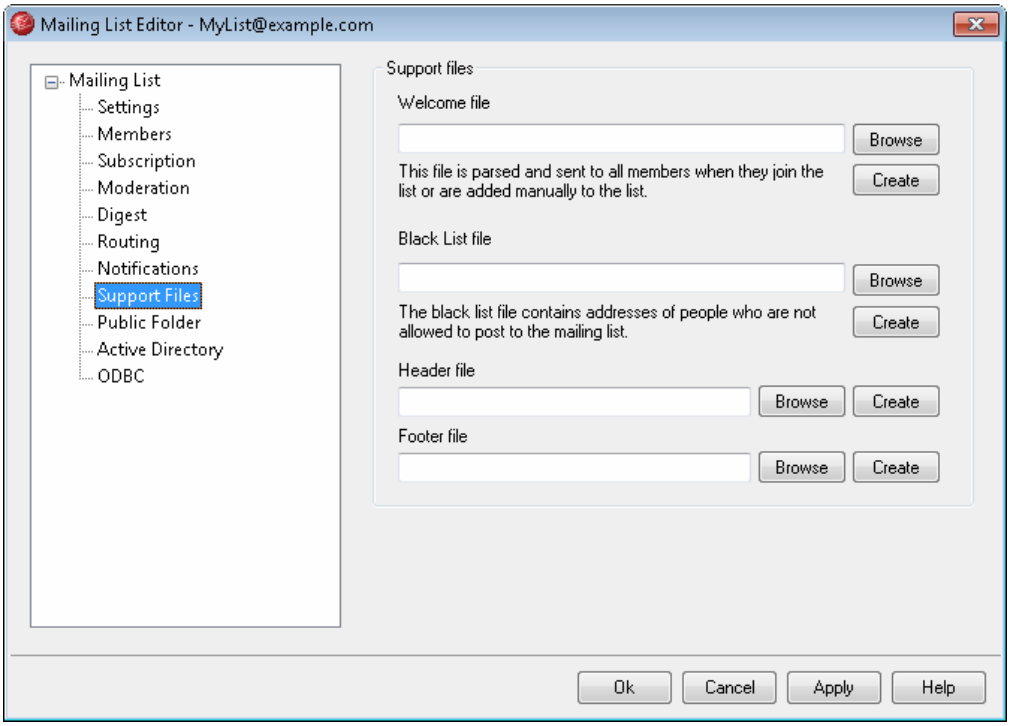
**Inform non-members that their message was refused**
When this option is enabled and non-members of a private list send mail to the list, MDaemon will inform them that the list is private. They will also be given instructions on how to subscribe to list. Lists are designated as private by using the *Only list members can post to this list* option located on Settings 431.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### Returned Mail

**List's SMTP 'Bounce' address**
Use this option to specify the address that should receive any "bounced" mail or deliver status notification messages generated from list traffic. Any given message to a mailing list with 100 recipients might have, for example, ten undeliverable addresses due to address changes, down servers, or the like. The SMTP system will generate and return to the sender of the message a notification message concerning these undeliverable conditions. Using this option you can designate the address that should receive these messages for your mailing lists. You can also choose for no one to receive them, in which case MDaemon will place list mail into the mail stream in such a way that return mail will not be possible. This address should NOT be the mailing list's address.

## 7.1.1.8 Support Files




### Support Files

**Welcome File**
If specified, the file listed here will be processed and have its contents emailed to all new members just after they subscribe. You may use the following macros in a new member welcome file:

| | |
|---|---|
| `$PRIMARYDOMAIN$` | This macro expands to MDaemon's Default Domain name, which is designated on the Domain screen 41. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| $PRIMARYIP$ | This macro will return the IP address associated with MDaemon's Default Domain. |
| $MACHINENAME$ | This macro returns the contents of the FQDN option designated on the Domain screen. |
| $LISTEMAIL$ | Displays the list's email address. Example: `MyList@example.com` |
| $LISTNAME$ | Displays the name of the mailing list. Example: `MyList` |
| $LISTDOMAIN$ | This macro returns the mailing list's domain. Example: `example.com` |
| %SETSUBJECT% | Use this macro to designate an alternate subject for the Welcome message. The designated subject text can include other list macros such as `$LISTEMAIL$`. Example: `%SetSubject %=Welcome to the $LISTNAME$ list.` |

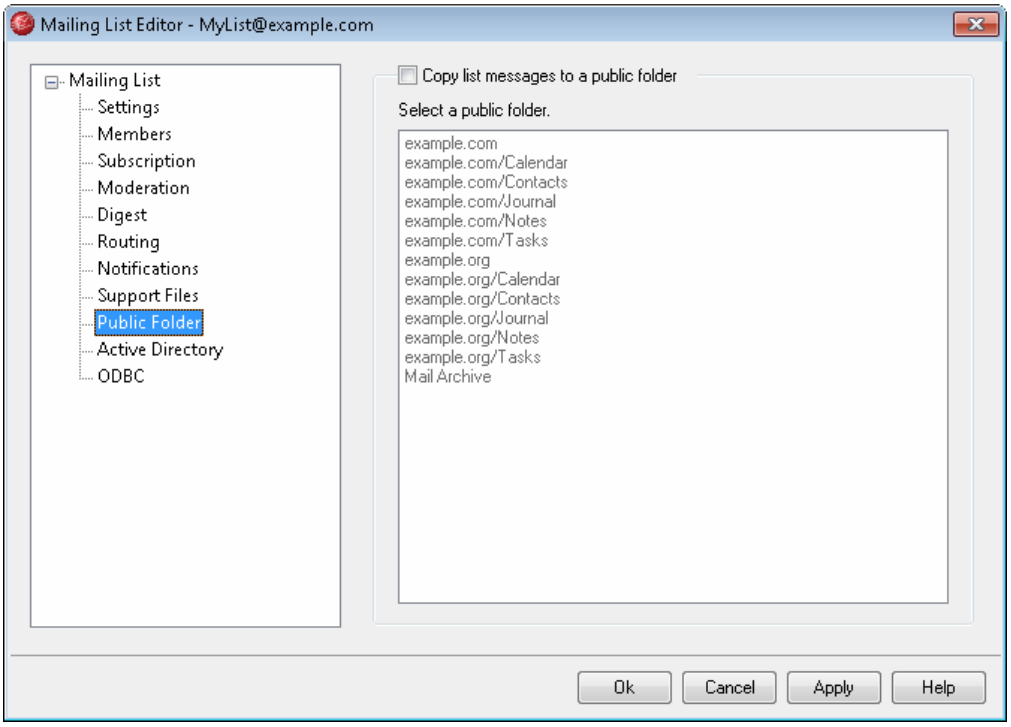
**Black List File**
If specified, the file listed here will be used to suppress messages sent from specified users.

**Header/Footer File**
The contents of the files specified here will be used as the header and/or footer file for list messages.

**Create**
To create a new file, click the *Create* button that corresponds to the file that you wish to create, specify a name, and then click *Open*. This will open the newly created file in Notepad for you to edit.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 7.1.1.9 Public Folder



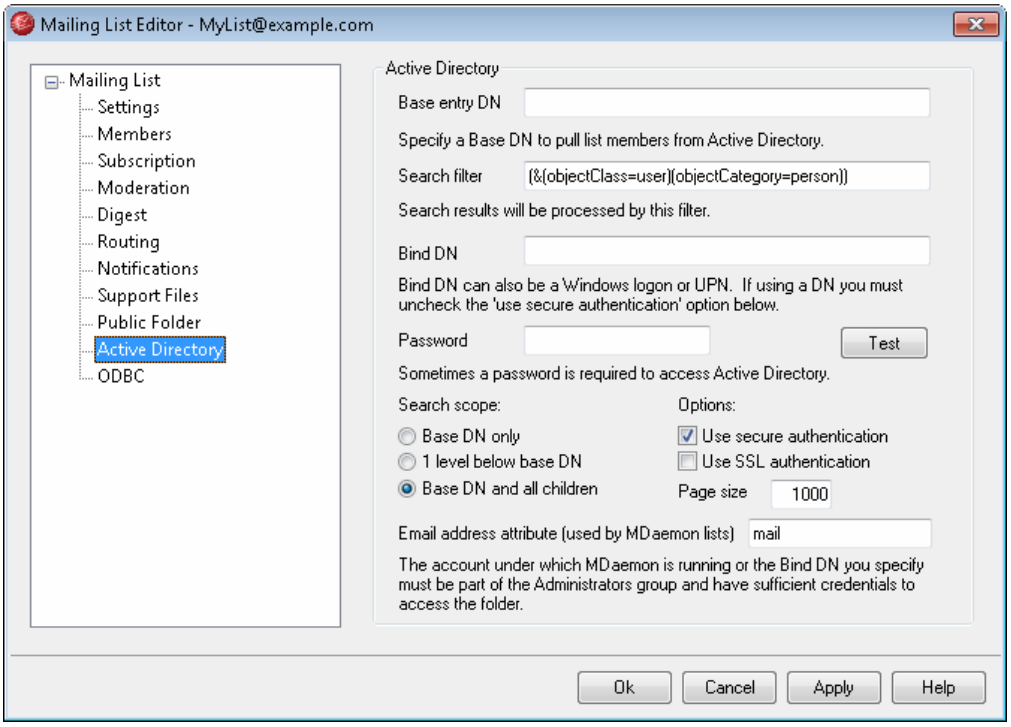

MDaemon supports using Public IMAP Folders[74] with mailing lists. Unlike personal IMAP folders, which are typically only accessible by a single user, Public folders are extra folders that are available to multiple IMAP users. The options on this screen are used to cause all messages destined for the Mailing List to be automatically copied to one of your public folders.

**Copy list messages to a public folder**
Enable this control if you want this list's messages to be copied to one of your Public Folders in addition to being delivered to the list.

**Select a public folder**
Click the Public Folder that you wish to associate with this list's messages.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 7.1.1.10 Active Directory




Use the options on this screen if you wish to pull some list member addresses from Active Directory.

#### Active Directory

**Base entry DN**
Specify the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search Active Directory for addresses. You can use "`LDAP://rootDSE`" in this option to begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts or desired group of addresses in your particular Active Directory tree can reduce the amount of time required to search the DIT. Leave this field blank if you do not wish to pull any list addresses from Active Directory.

**Search filter**
This is the LDAP search filter that will be used when for searching Active Directory. Use this filter to enable MDaemon to more precisely locate the desired user accounts or addresses that you wish to treat as list members.

**Bind DN**
This is the DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

**Password**
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

**Test**
Click this button to your Active Directory configuration.

### Search scope:

This is the scope or extent of your Active Directory searches.

**Base DN only**
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

**1 level below base DN**
Use this option if you wish extend your Active Directory search to one level below the supplied DN in your DIT.

**Base DN and all children**
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

### Options:

**Use secure authentication**
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

**Use SSL authentication**
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

**Page size**
If the results of an Active Directory query exceed a specified number of entries, then they will be returned in separate "pages" in order to retrieve all the results. This setting is the maximum number of entries that will be included per page.

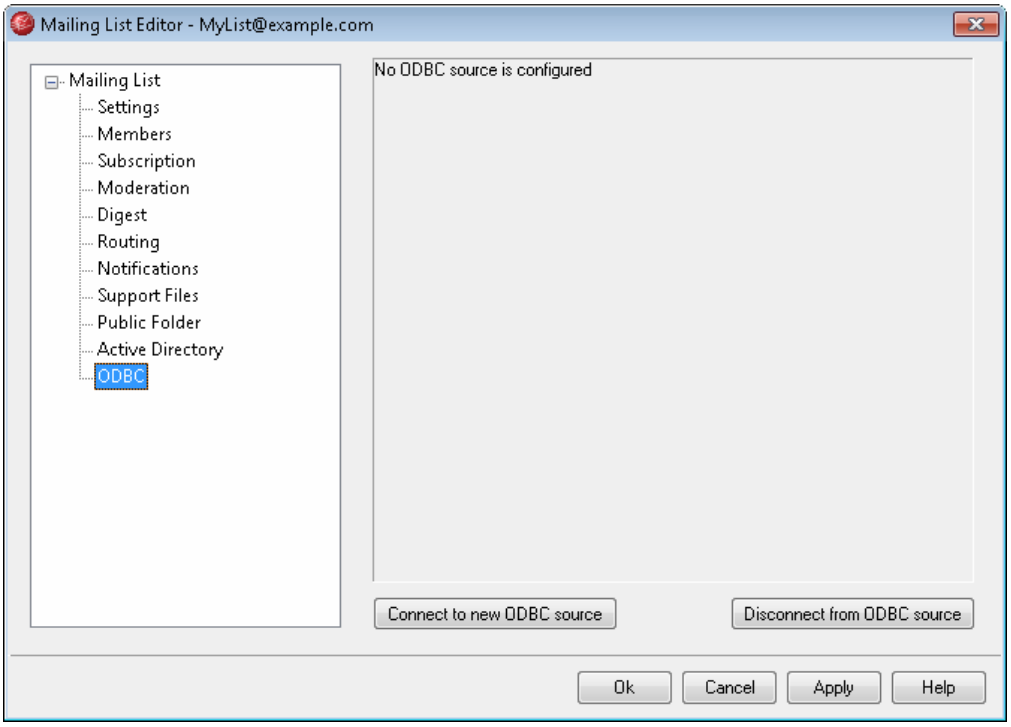
Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Email address attribute**

You must use this field to specify the attribute that will contain the email addresses used by this list. For example, if you used "`Mail`" in this field, then each Active Directory account that you wish to be treated as a list member must have the "`Mail`" attribute, and that attribute must contain an email address.

### 7.1.1.11 ODBC




Using this feature you can maintain the list's membership list in an ODBC compliant database. The ODBC screen of the Mailing List editor is used to select a data source, table, and field mappings for MDaemon to link to the list. When messages arrive for your list one or more SQL queries will be performed automatically and the resulting email addresses will be treated as part of the list's membership.

You can add, remove, and modify members of your list in the database using whatever ODBC compliant database application you choose.

**ODBC**

This section displays the current ODBC properties that you have set up for the mailing list. It displays the database's field mappings and the SQL queries that you have configured to designate each member's membership status (i.e. Normal, Post Only, Read Only, and/or Digest mode).

**Connect to new ODBC source**
Click this button to open the ODBC Selector Wizard for choosing the system data

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

source that you wish to use for the mailing list.

**Disconnect from ODBC source**
Click this button to disconnect the list from the ODBC data source listed in the space above.

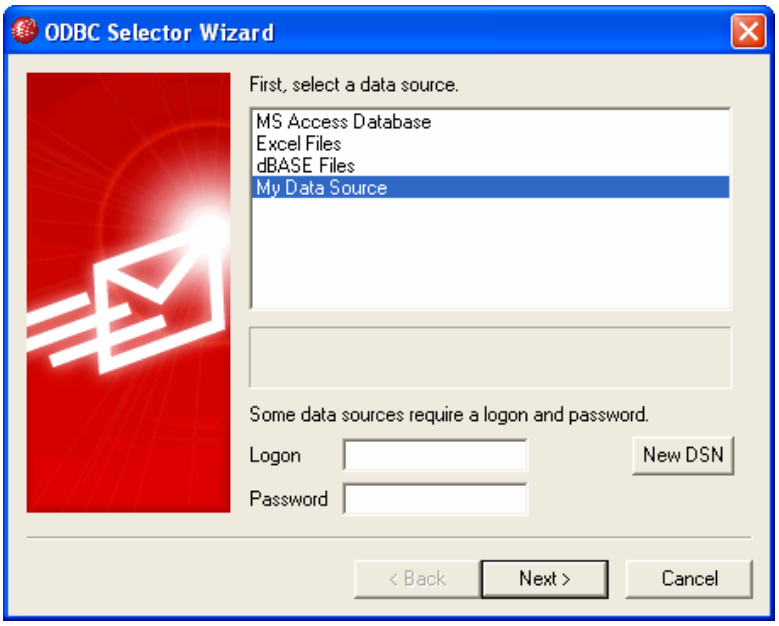
**See:**

**Configuring an ODBC System Data Source for a Mailing List** 451
**Creating a New System Data Source** 453

### 7.1.1.11.1 Configuring an ODBC Data Source

To use an ODBC accessible database with a mailing list:

1. On the ODBC screen 450 of the Mailing List editor, click Connect to new ODBC source to open the ODBC Selector Wizard.




2. Select the data source that you wish to use for the list. If there is not a compatible data source listed, click New DSN and then follow the instructions listed under, **Creating a New ODBC Data Source** 453.

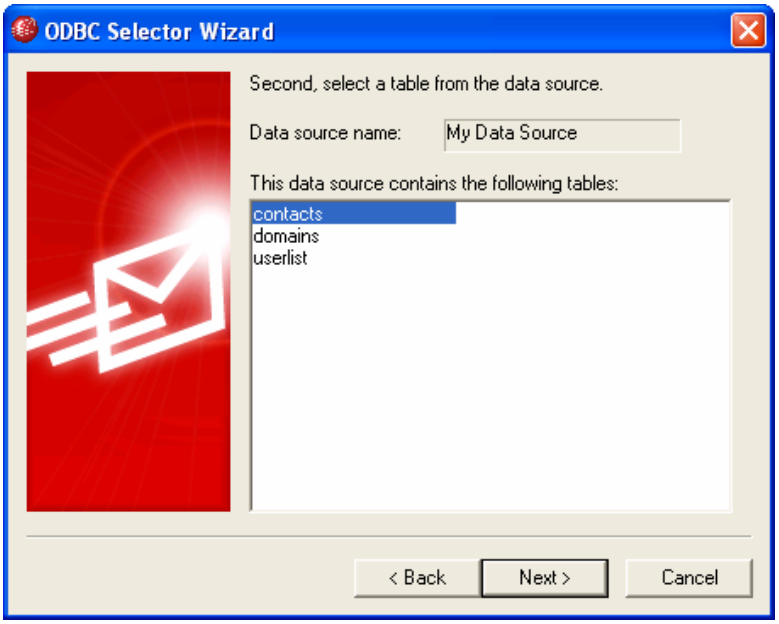
3. If required, enter the data source's Logon and Password.

4. Click Next.

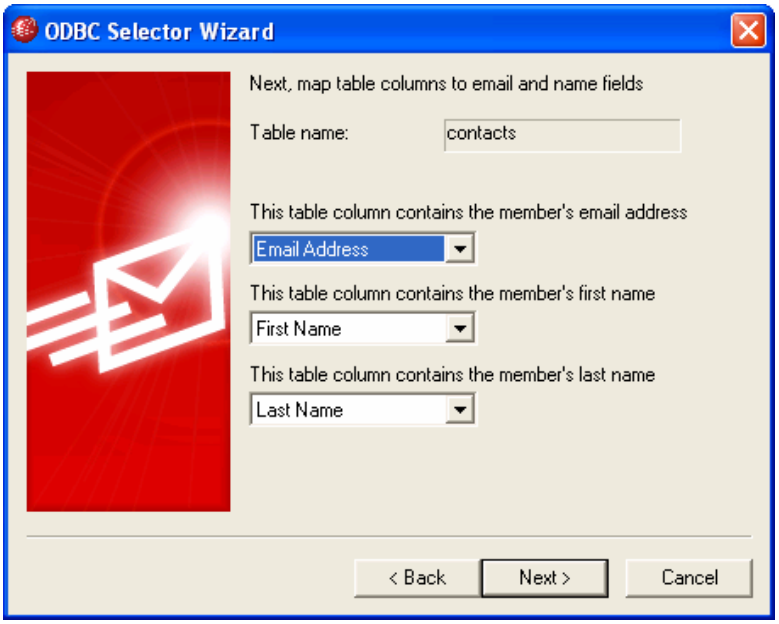
5. The data source must contain at least one table with fields for email addresses and names. If the data source contains one or more qualifying tables, choose the desired table and click Next. Otherwise, click Cancel to exit the ODBC Selector Wizard and then use your database application to add a table to the relevant

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

database before continuing.



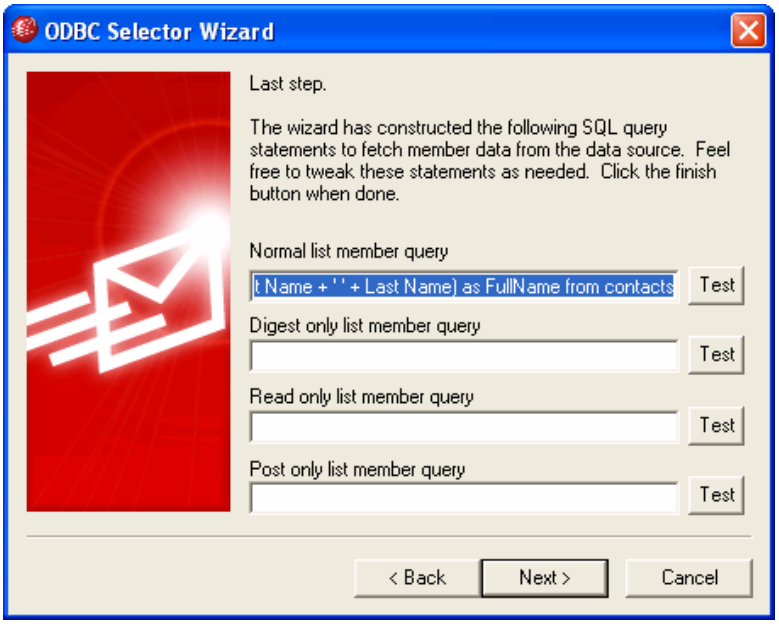

6. Use the drop-down list boxes to designate the table fields that will correspond to **email address**, **first name**, and **last name**. Click Next.




7. The ODBC Selector Wizard will construct an SQL query statement based on your selections in **Step 6**. MDaemon will use it to retrieve normal list member data from your database. You can edit this statement as desired, and include other query statements in the remaining controls to cause members to receive messages in Digest mode, and to designate members as Read Only or Post Only. A Test button is provided beside each control so that you can test your query statements to make sure they retrieve the proper data. When you are finished configuring your

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

query statements, click Next.




8. Click Finish.

---

**See:**

**Mailing List Editor » ODBC** 450
**Creating a New ODBC Data Source** 453

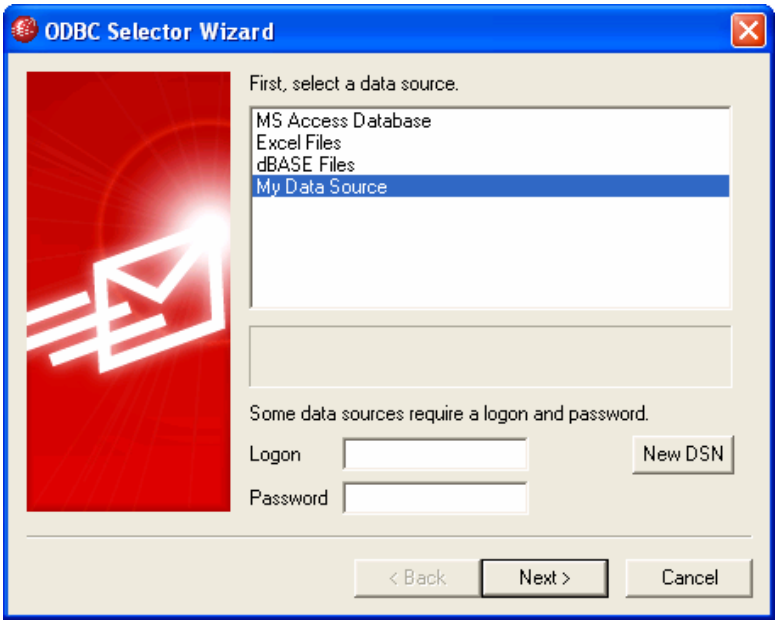
### 7.1.1.11.2 Creating a New ODBC Data Source

To create a new ODBC system data source for use by a mailing list:

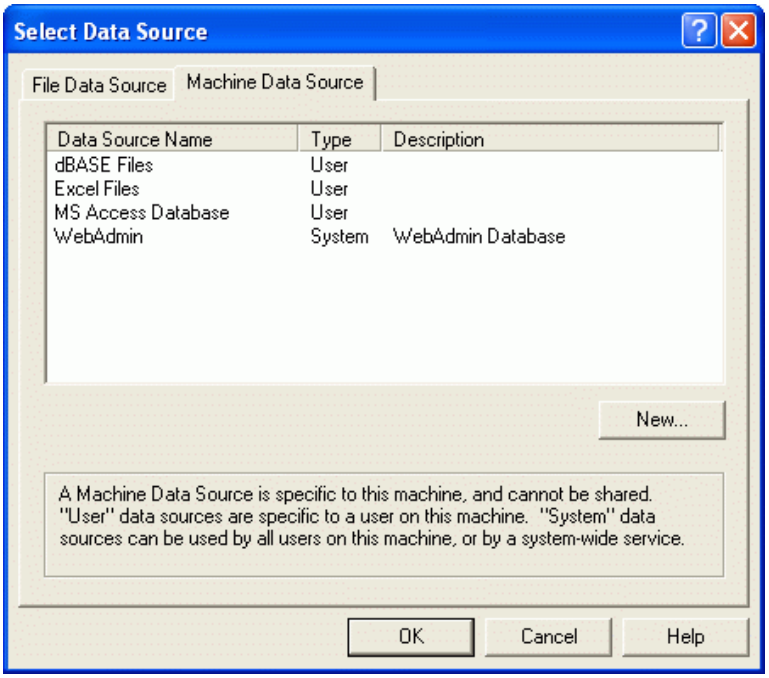
1. On the ODBC screen 450 of the Mailing List editor, click Connect to new ODBC source to open the ODBC Selector Wizard.

2. Click New DSN to open the Select Data Source dialog.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

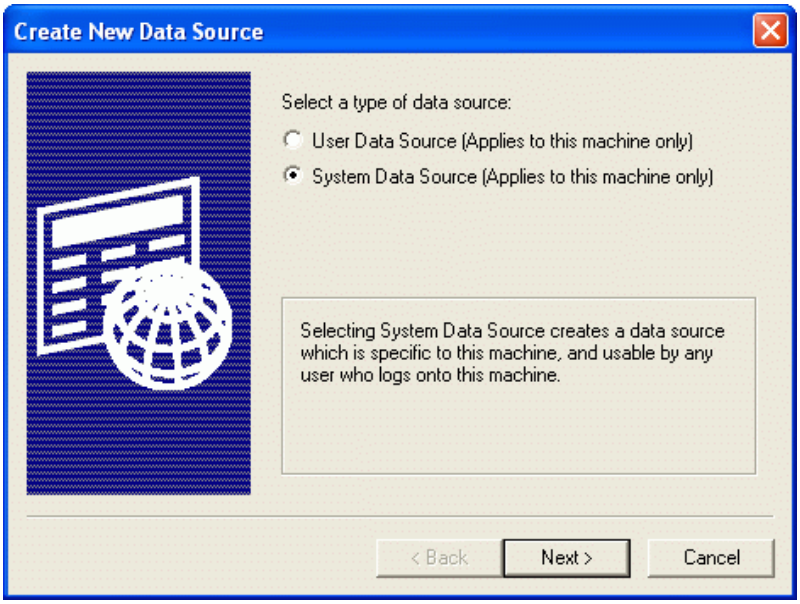



3. Switch to the Machine Data Source tab, and click New... to open the Create New Data Source dialog.

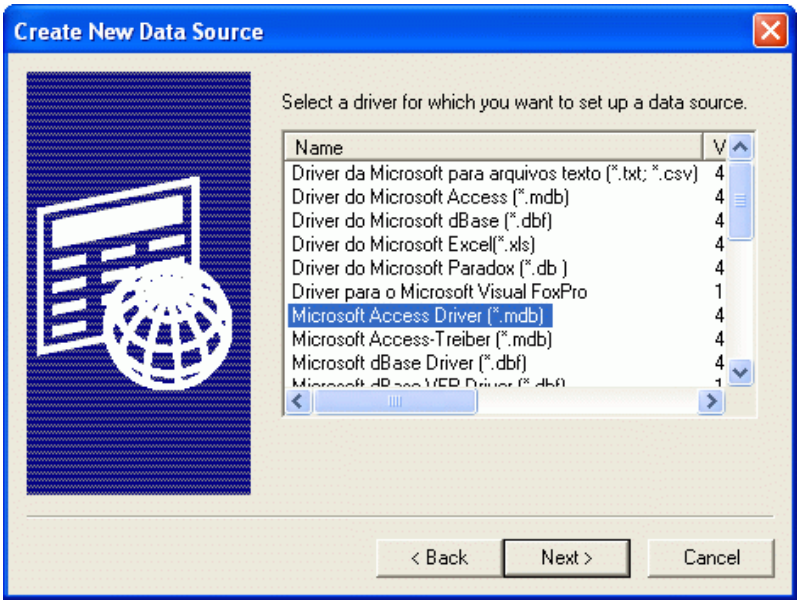



4. Select System Data Source, and click Next.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

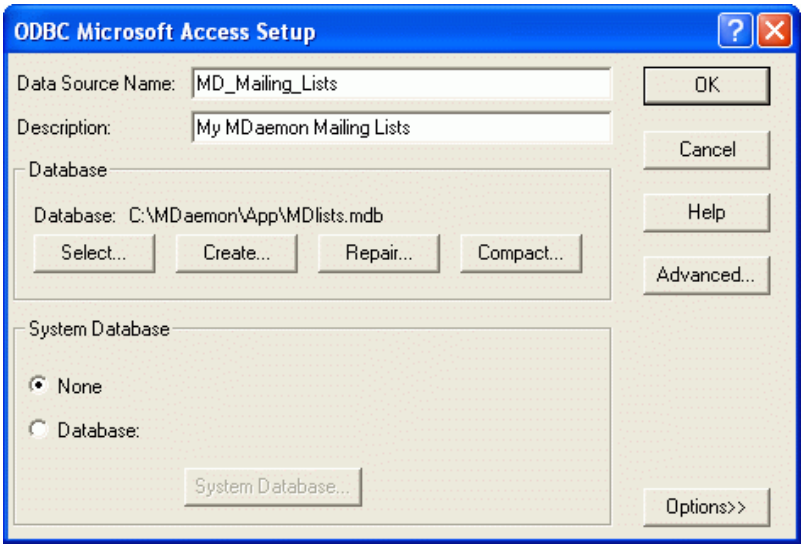



5. Select the database driver for which you wish to set up the data source, and click Next.




6. Click Finish to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.




7. Designate a Data Source Name for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click OK to close the driver-specific dialog.

9. Click OK to close the Select Data Source dialog.

**See:**

**ODBC - Mailing Lists** 450
**Configuring an ODBC System Data Source for a Mailing List** 451

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# Section VII

# 8 Gateways Menu

## 8.1 Domain Gateways

The Gateway Editor[459] is an MDaemon PRO feature and is reached from the Gateways » New Gateway... or Gateways » Edit Gateway... menu selection. This feature provides a limited yet useful secondary level of support for hosting multiple domains or acting as a backup mail server for someone.

For example:

> Suppose you wish to act as a backup server or mail-drop for a third party, receiving its incoming email and storing it in a folder on your server, but you do not wish to host its domain fully, maintaining its individual user accounts. Let's use "example.com" as its name.
>
> The first thing you will do is enter "example.com" in the *Domain name* option on the Domain screen. Then, you will select the storage folder where incoming mail will be stored for the domain. All mail that MDaemon receives for that domain will be separated from the main mail stream and placed in that folder, regardless of the specific individuals to which each message is addressed.
>
> Next, you will designate the collection or delivery methods that you wish to allow or use to get the domain's email to its actual email server, where its user accounts are hosted. There are three ways to do this: use the *Deliver stored messages each time MDaemon processes remote mail* option on the Domain screen[460], use the Dequeuing[466] options, or set up an account for the domain on the Account screen[468].
>
> Finally, you will likely have to edit the DNS settings for example.com so that your MDaemon server is a designated MX host for that domain.

There are many other features and options available to gateways, but the above example is the basic form that a typical gateway will take. If, however, you require an atypical configuration then you may have to do some things differently, such as when you wish to use a domain name that doesn't actually exist on the Internet, like "company.mail." Receiving messages for an otherwise invalid domain name such as that is possible, but the domain name must be "hidden" inside a Default Domain[41] address. Using that method, addresses can be constructed that will pass through the default domain and on to the gateway. For example, if your default domain is example.com and you have a gateway for company.mail, then someone could send a message to "bob@company.mail" by using the address, "bob{company.mail}@example.com." Since "example.com" is the registered domain hosted by MDaemon, this message would be delivered properly, but when MDaemon received the message in that format it would convert the address to "bob@company.mail" and deliver the message to the folder specified for that gateway. Of course the simplest method is still to register a valid domain name for the gateway and then point its DNS or MX record to example.com.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**Gateway Editor** 459
**Default Domain** 41
**Domain Manager** 108

## 8.1.1 Gateway Editor

The Gateway Editor is reached by clicking the Gateways » New Gateway... or Gateways » Edit Gateway... menu selection on MDaemon's menu bar. It includes the following screens:

**Domain** 460
Use this dialog to designate the domain name for which MDaemon will be acting as a backup server or gateway. This is also where you will designate the folder used for storing the domain's messages.

**Verification** 461
If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, you can use this dialog to specify that server and thus verify the validity of recipient addresses of incoming messages. When a recipient address is found to be invalid the message will be rejected. With this method you can avoid having to assume that all recipients of a domain's messages are valid.

**Forwarding** 465
With this dialog you can declare a host or address to which the domain's mail will be forwarded as soon as it arrives. There are also options for stating whether a copy of these messages should be kept locally and for designating the port on which the forwarded messages should be sent.

**Dequeuing** 466
Using the options on this dialog, you can configure MDaemon to respond to ETRN and ATRN requests made on behalf of the domain in order to dequeue its messages. You can also configure several other dequeuing related options.

**Account** 468
Here you can create a POP3 or IMAP user account that will have access to this domain's stored mail. Using the name and password that are assigned here, a mail user agent (MUA) such as an ordinary email client or another MDaemon server can access the domain's mailbox and collect its mail.

**Quotas** 469
This dialog is used for assigning a limit to the amount of disk space that the domain may use and the maximum number of messages that may be stored.

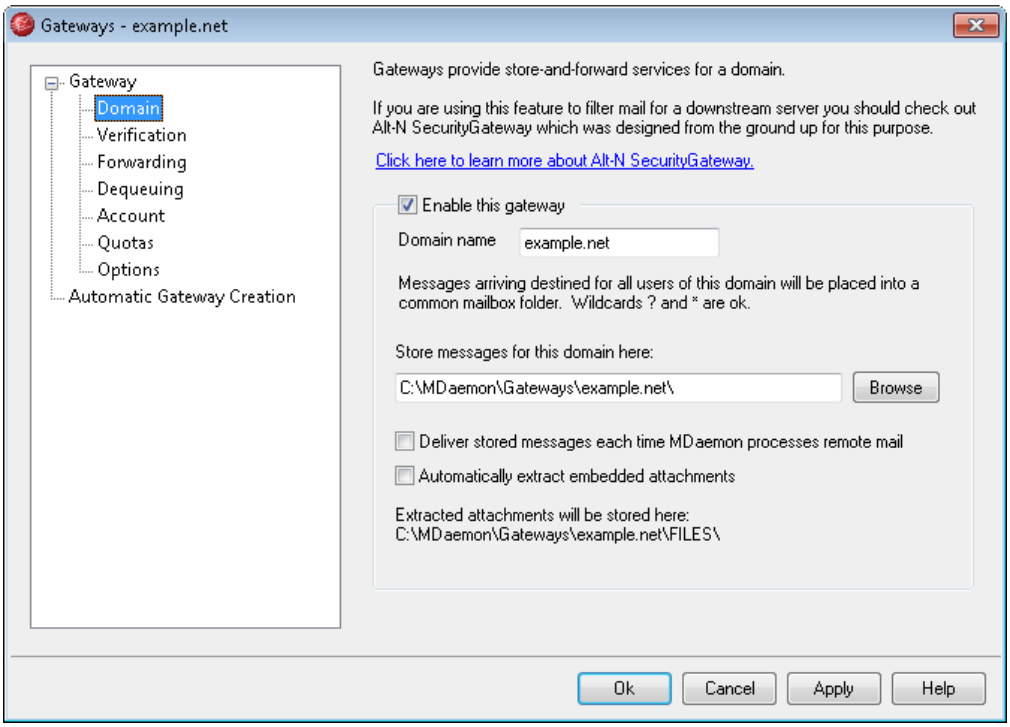
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Options**[470]
This screen contains a number of other options that will apply to the selected domain gateway. For example, you can enable/disable AntiVirus and AntiSpam scanning for the gateway, designate whether or not authentication is required when dequeuing mail, designate an authentication password, designate IP address connection restrictions, and several other options.

**See:**

**Domain Gateways**[458]

### 8.1.1.1 Domain




#### Gateway Domain

**Enable this gateway**
Check this box to enable the domain gateway.

**Domain name**
Enter the name of the domain for which you wish MDaemon to act as an email gateway or mail drop.

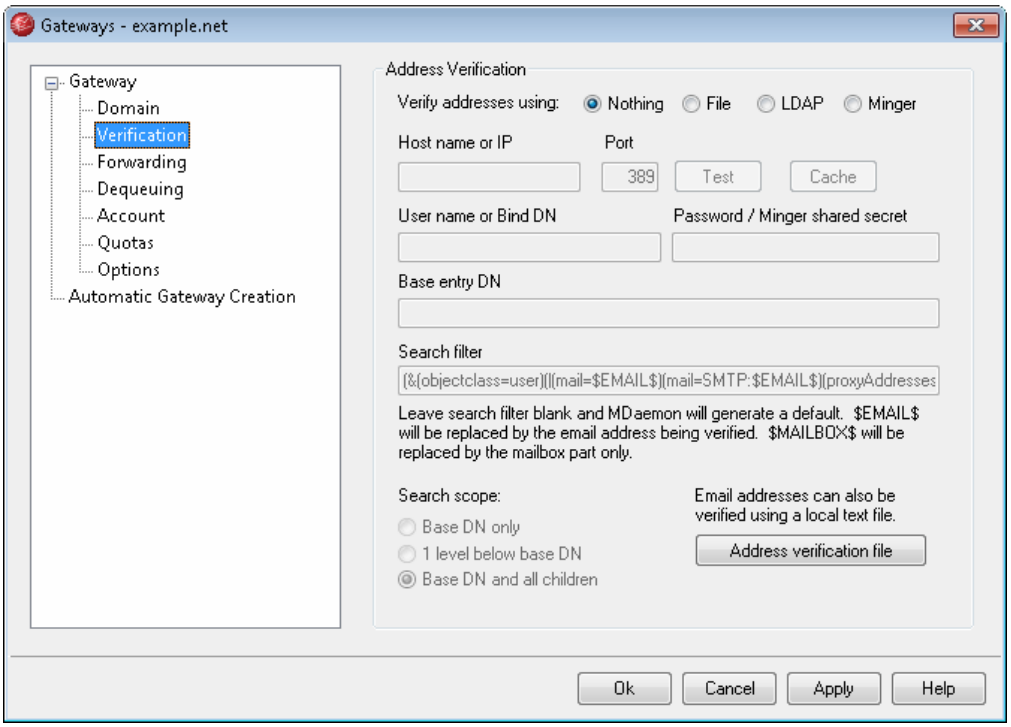
**Store messages for this domain here**
Enter the directory where you wish to store incoming mail for the domain. All of its messages will be stored in the same folder regardless of the individual recipients to which each message is addressed.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Deliver stored messages each time MDaemon processes remote mail**
Ordinarily, when MDaemon receives mail that is intended for one of its gateways, it will store the mail until that domain connects to MDaemon to collect it. In some situations you may want MDaemon to attempt to deliver the mail directly via SMTP rather than waiting for the domain to collect it. When this option is enabled, MDaemon will attempt to deliver the domain's messages each time remote mail is processed. The gateway's mailbox will temporarily act as a remote queue and delivery will be attempted. Any messages that cannot be delivered will simply remain in the gateway's mailbox until they are collected by the domain or are successfully delivered later; they will not be moved into the remote queue or retry system. However, if you do not have the domain's DNS properly configured, or if you have your MDaemon configured to pass all outgoing messages to some other host for delivery, then you could cause those message to get caught in a mail loop and then eventually be treated as undeliverable.

**Automatically extract embedded attachments**
Some mail systems require attached files be extracted before submission of mail messages to the mail stream. To facilitate this, MDaemon can auto-extract incoming MIME attachments and place them in the `\Files\` subfolder underneath the domain's message folder. Check this box if you wish to automatically extract attachments.

### 8.1.1.2 Verification




One common problem with domain gateways and mail-drops is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if you act as a gateway for `example.com` and a message comes

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

for user01@example.com then you have no way of knowing whether or not there is actually a mailbox, alias, or mailing list corresponding to that address on example.com's email server. Thus you have no choice but to assume that the address is valid and accept the message. Further, since spammers commonly send messages to many invalid addresses, this problem can result in large amounts of junk email be accepted for the gateway.

MDaemon contains a method to prevent this by verifying the recipient addresses. If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, then you can use the options on this screen to specify the LDAP, Active Directory, or Minger server where this information is stored. Then, when a message arrives for example.com, you can lookup the recipient's address on the other server and discover whether or not it is valid.

### Address Verification

**Verify addresses using:**

**Nothing**
Choose this option if you do not wish to use email address verification for this domain gateway. MDaemon will treat all of the domain's incoming messages as if the recipient is a valid address, since it will have no way of identifying which addresses actually exist for that domain.

**File**
Choose this option if you wish to use the GatewayUsers.dat file as the definitive list of addresses that will be used to verify whether or not the recipient of an incoming message for this domain is valid. This is a global list of addresses, applicable to all of your domain gateways, and even if you have chosen to use one of the other verification methods, this list will still be used as an extra source of valid addresses. When using the *File* option, however, it will be the only verification option used. You can open and edit the valid address list by clicking the *Address verification file* button below.

**LDAP**
Choose this option to activate remote address verification via LDAP or Active Directory. Whenever a message arrives for the remote domain its LDAP or Active Directory server will be queried to determine whether or not the recipient is valid. If it isn't valid the message will be rejected. If MDaemon is unable to connect to the LDAP/AD server then it will assume the address is valid.

**Minger**
Choose this option if you wish to query the domain's Minger server to verify recipient addresses for this domain. If MDaemon is unable to connect to the server then it will assume the address is valid. There is also a global option located on Options 470 that you can use to cause MDaemon to query your Domain Sharing 64 hosts as well.

**Host name or IP**
Enter the host name or IP address of the domain's LDAP/Active Directory or Minger server. This is the LDAP/AD or Minger server to which MDaemon will connect in order

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

to verify that the recipient of an incoming message is a valid address at the domain for which this MDaemon is acting as a gateway or backup server.

**Port**
Specify the port that the domain's LDAP/AD or Minger server is using. MDaemon will use this port when verifying address information via LDAP, Active Directory, or Minger.

**Test**
Click this button to test whether or not you have the remote address verification settings configured properly. MDaemon will simply attempt to connect to the designated LDAP/AD server and verify that it responds to the specified information.

**Cache**
Click this button to open the LDAP/Minger cache. You can enable/disable the cache on Options 470.

**User name or Bind DN**
Enter the User name or DN of the account that has administrative access to the domain's LDAP/AD server so that MDaemon can verify the recipients of incoming messages addressed to the domain for which it is acting as a gateway or backup server. This is the DN used for authentication in the bind operation.

**Password or Minger shared secret**
This password will be passed to the domain's LDAP/AD server along with the *Bind DN* value for authentication. If using a Minger server then this is the shared secret or password used.

**Base entry DN**
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will query your LDAP/AD server for address verification.

**Search filter**
This is the LDAP/AD search filter that will be used when querying your server to verify addresses. MDaemon will setup a default search filter that should work in most cases.

### Search scope:

This is the scope or extent of your LDAP/AD searches.

**Base DN only**
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

**1 level below base DN**
Use this option if you wish to extend your LDAP/AD search to one level below the supplied DN in your DIT.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Base DN and all children**
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

**Address verification file**
Click this button to open the Gateway Valid Email Address List (i.e. the `GatewayUsers.dat` file). This contains a list of addresses that MDaemon will consider to be valid recipients for incoming messages addressed to your domain gateways. Regardless of the verification option selected above, MDaemon will use this list as an extra source of valid address data. When using the *File* option above, however, it will be the definitive and only verification option used.

## Using multiple configurations for LDAP verification queries

You can specify multiple LDAP configurations for your gateway domains. To specify extra sets of LDAP parameters, setup your first set normally and then manually edit the `GATEWAYS.DAT` file using Notepad.

Your new set of parameters should be created using the following format:

```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

For each new set of parameters, increase the numeral in each parameter's name by 1. For example, in the sample set above, each parameter's name ends with "1". To create an additional set each name would end with "2". In another set, each would end "3", and so on.

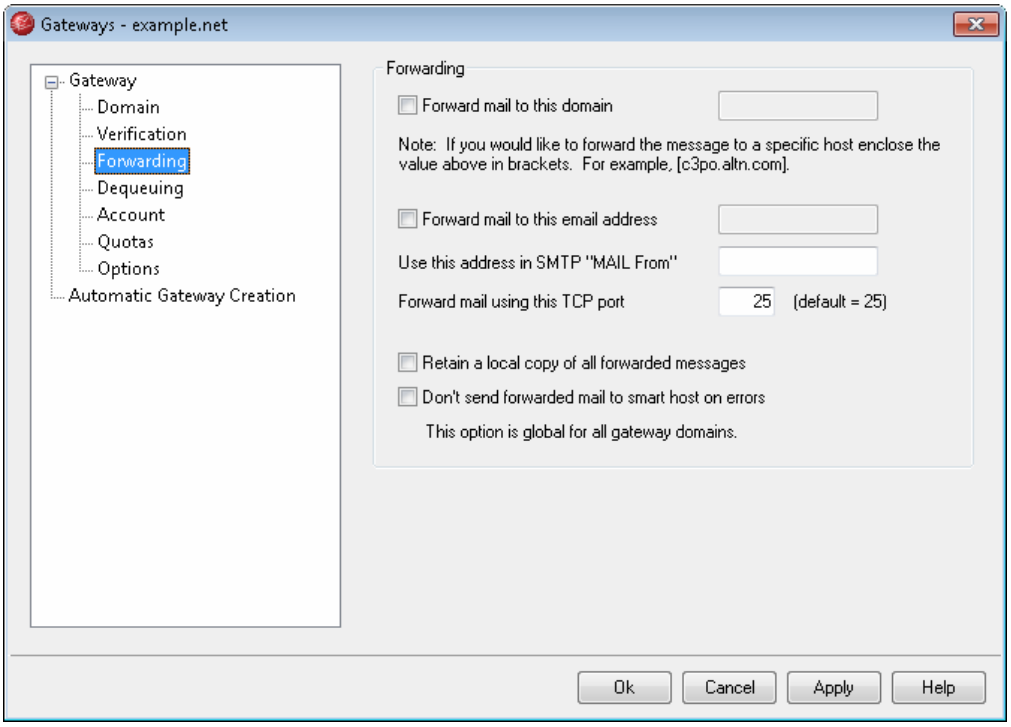
When the LDAP queries take place, MDaemon will perform multiple LDAP queries in sequence to find a match. If an error or a match is found no further checks are performed.

**See:**

**LDAP/Address Book Options** 96
**Minger** 422

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 8.1.1.3 Forwarding




#### Forwarding

**Forward mail to this domain**
Sometimes it is advantageous to simply forward a copy of all messages for a domain as they arrive. If you wish to configure MDaemon to do this, enter the name or IP address of the domain to which copies of incoming mail for this domain should be sent. If you wish to forward the messages to a specific host then place the value in brackets (for example, `[host1.example.net]`).

**Forward mail to this email address**
Use this feature if you wish to forward to a specific email address all email messages destined for this client domain.

**Use this address in SMTP "MAIL From"**
MDaemon will use this address in the SMTP "Mail From" transaction.

**Forward mail using this TCP port**
MDaemon will forward this mail using this TCP port.

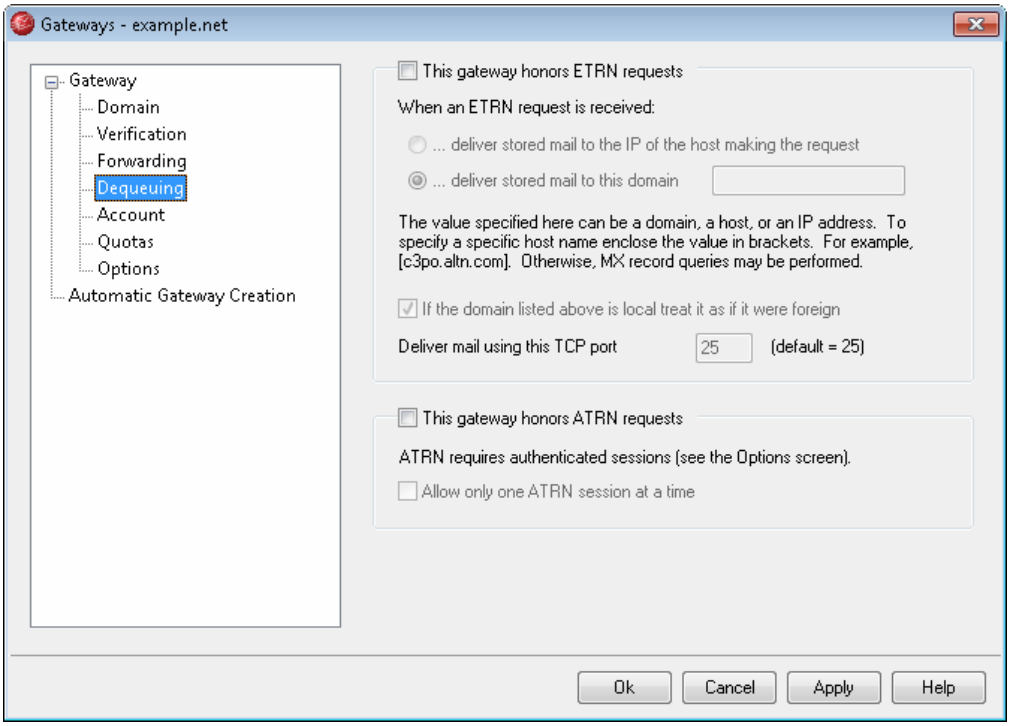
**Retain a local copy of all forwarded messages**
Select this option if you wish MDaemon to retain an archival copy of each message locally once it has been forwarded.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Don't send forwarded mail to smart host on errors**
Click this option to prevent the sending of forwarded emails to the host specified above when delivery errors occur.

This is a global setting applying to all domain gateways, and it is disabled by default.

### 8.1.1.4 Dequeuing




**ETRN**

**This gateway honors ETRN requests**
When this switch is enabled MDaemon will respond to ETRN requests made by qualified hosts on behalf of the domain for which MDaemon is acting as an email gateway. The ETRN command is an SMTP extension that signals a server storing mail for a particular domain that it is time to begin spooling the mail. When MDaemon receives an ETRN request for a domain, it will immediately begin spooling the stored mail for delivery using subsequent SMTP transactions. Please note that the SMTP session that issues an ETRN request will not be the one that receives any stored mail. MDaemon will use subsequent independent SMTP transactions to send any mail it has stored for the domain. This preserves the message envelope and is more secure. Also note that the host to which MDaemon will spool any stored mail may not immediately begin reception of these messages. ETRN only guarantees that any stored mail is *spooled* for delivery. The actual *process* of delivery is subject to other

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

administrator-imposed restrictions and may have to wait in the outbound mail queue for the next scheduled remote mail processing event to take place. Because of these limitations we recommend using On-Demand Mail Relay (ODMR) 59 and its ATRN command rather than ETRN. This method is not supported by all clients and servers, however, and will therefore only be available to client domains using a server that does so. MDaemon fully supports ODMR on both the client and server side.

By default MDaemon requires that the connecting host issuing the ETRN request first authenticate itself via ESMTP AUTH using the *Domain name* 460 and *Gateway AUTH password* 470 as its login credentials. If you do not wish to require authentication than you can disable it on Options 470 by clearing *ETRN dequeuing requires authentication*.

### When an ETRN request is received:

**...deliver stored mail to the IP of the host making the request**
Selecting this option will cause MDaemon to send any stored mail to the IP address of the machine that made the ETRN request. The requesting machine must be running an SMTP server to receive these messages.

**...deliver stored mail to this domain**
This is the host name, domain name, or IP address to which any stored mail will be sent when an ETRN request is received and honored. The receiving machine must be running an SMTP server to receive these messages. Note: when a domain name is specified in this option, A and MX records may be used, depending on the DNS results during delivery. If you wish to deliver the messages to a particular host then place the host name in brackets (for example, `[host1.example.net]`) or specify an IP address instead of a domain name.

**If the domain listed above is local treat it as if it were foreign**
Activate this control if the domain is local but you want its mail to be spooled as if it is remote.

**Deliver mail using this TCP port**
Use this box to specify the port on which the domain's mail will be spooled.

### ATRN

**This gateway honors ATRN requests**
Enable this option if you want MDaemon to respond to `ATRN` commands from the gateway's domain. `ATRN` is an ESMTP command used in On-Demand Mail Relay (ODMR) 59, which is currently the best relay method available for mail hosting. It is superior to ETRN and other methods in that in requires authentication before mail is dequeued and does not require a static IP address. A static IP address isn't required because the flow of data between MDaemon and the client domain is immediately reversed and the messages are de-spooled without having to make a new connection, unlike `ETRN`, which uses a separate connection after the `ETRN` command is sent. This enables client domains with a dynamic (non-static) IP address to

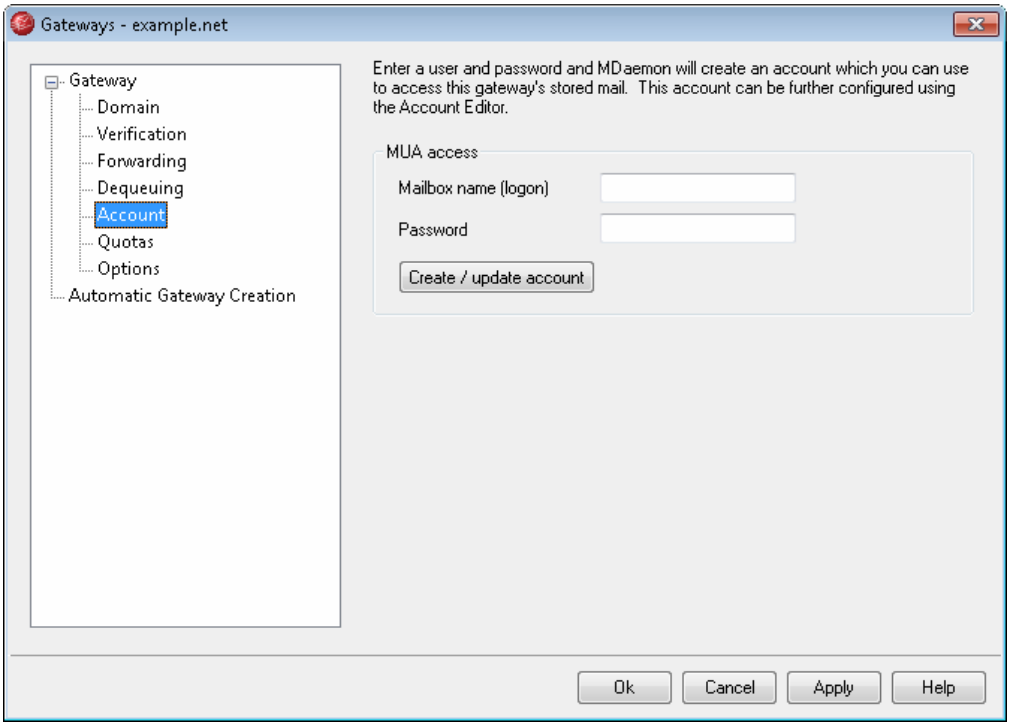
Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

collect their messages without having to use POP3 or DomainPOP, because the original SMTP envelope is preserved.

ATRN requires a session using the AUTH command. You can configure the authentication credentials on the Options 470 screen.

**Allow only one ATRN session at a time**
Click this check box if you wish to restrict ATRN to one session at a time.

### 8.1.1.5 Account




You can use this screen to create an MDaemon account that will be associated with this gateway. By using this account, an email server or mail client can then connect to MDaemon to collect the gateway's messages via IMAP, DomainPOP, or POP3. IMAP is only available in MDaemon PRO.

**Mailbox name (logon)**
Enter the mailbox name (i.e. the user account name) that the client will use to access the gateway's messages stored in its mailbox.

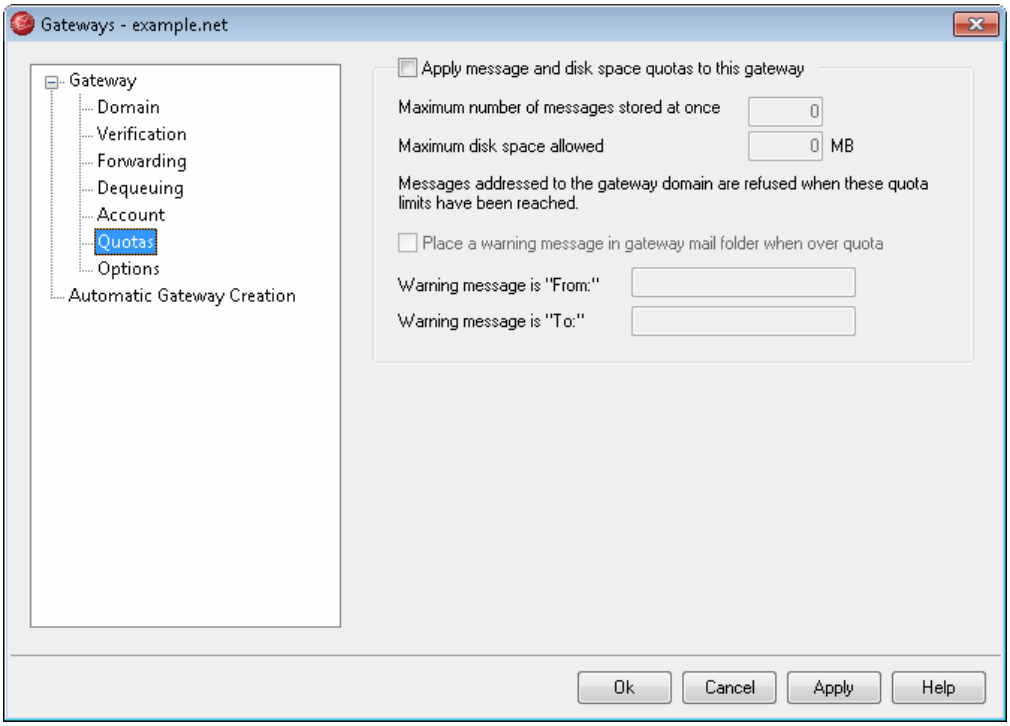
**Password**
Enter the password that the client's domain will use to access the messages stored in its mailbox.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Create/update account**
Click here to create an account or to update the Mailbox name and Password values if the account already exists.

You can edit (or even remove) an account using the Account Manager340. Be careful if you remove an account because that will delete its mail and folders, which are also used by the gateway.

### 8.1.1.6 Quotas




**Quotas**

**Apply message and disk space quotas to this gateway**
Enable this option if you wish to designate a maximum number of messages allowed to be stored for the domain or a maximum amount of disk space (in kilobytes) that it can use. This includes any decoded file attachments in its Files directory. When a quota is reached, any further incoming messages addressed to the domain will be refused.

**Maximum number of messages stored at once**
Use this box to designate the maximum number of messages that MDaemon will store for this gateway domain. Use "0" in this option if you do not wish to limit the number of messages.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

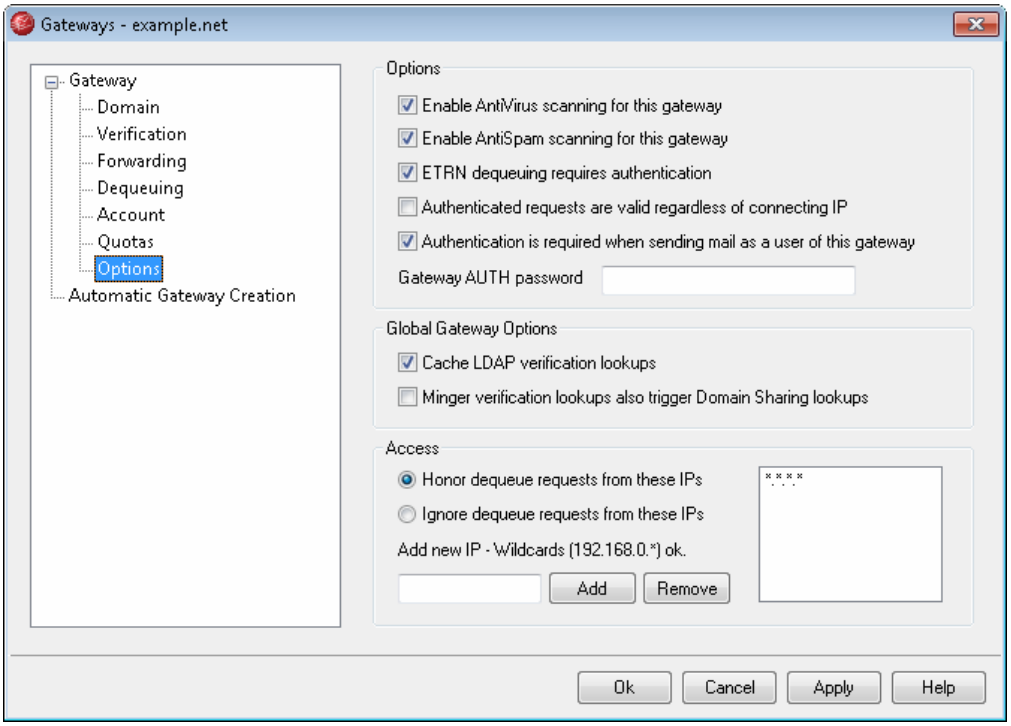
**Maximum disk space allowed**
Specify the maximum allowed disk space here. When messages and files stored for the domain reach this limit, any further incoming messages for the domain will be refused. Use "0" if you do not wish to set a disk space limit.

**Place a warning message in gateway mail folder when over quota**
If this option is enabled and a mail delivery to the domain is attempted that would exceed the maximum message or disk space limitations, an appropriate warning message will be placed in the domain gateway's mail folder. You can designate the warning message's "`From:`" and "`To:`" headers below.

**Warning message is "From:"**
Use this option to specify the "From:" address that will be used in the over-quota warning messages.

**Warning message is "To:"**
Use this option to specify the "To:" address that will be used in the over-quota warning messages.

### 8.1.1.7 Options




**Options**

**Enable AntiVirus scanning for this gateway**
Click this option if you have installed SecurityPlus for MDaemon and want this domain gateway's messages to be scanned. If you clear this option then

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

SecurityPlus will not scan this gateway's messages.

**Enable AntiSpam scanning for this gateway**
Click this option if you want to apply the Spam Filter settings to this domain gateway's messages. Otherwise, they will be excluded from Spam Filter scanning.

**ETRN dequeuing requires authentication**
When you configure the settings on the Dequeuing tab to accept ESMTP ETRN requests, this option will be used by default to require the connecting host to first authenticate using the ESMTP AUTH command. When this option is enabled, you must designate an authentication password in the "Auth password" box provided below.

Clear this checkbox if you do not wish to require authentication of hosts making ETRN requests.

**Authenticated requests are valid regardless of connecting IP**
Enable this checkbox if you wish to honor authenticated requests regardless of the IP address from which they are coming. If this control is not enabled then only requests from those IP addresses specified in the Access section will be honored.

**Authenticated is required when sending mail as a user of this gateway**
Click this check box if you want all messages claiming to be from this domain to require authentication. If a message is purported to be from this domain then it must be using an authenticated connection (or connecting from a Trusted IP address) or it will be refused. This option is enabled by default.

When new domain gateways are created, this option will be enabled by default. If you wish to change the default setting so that new gateways will have this option disabled, then edit the following key in the `MDaemon.ini` file:

```
[Special]
GatewaySendersMustAuth=No (default is Yes)
```

**Gateway AUTH password**
When using ATRN to dequeue this gateway's mail, or when you are requiring authentication via the *ETRN dequeuing requires authentication* option above, designate the gateway's AUTH password here.

The domain for which MDaemon is acting as an email gateway must use its domain name as the logon parameter. For example, if the domain gateway is "example.com" and is using ATRN to dequeue its mail, then it would authenticate using the login credentials "example.com" and the password specified here.

## Global Gateway Options

The following options are global options. They aren't limited to strictly this domain.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Cache LDAP verification lookups**
Click this checkbox if you wish to cache the results of LDAP verification[461] queries for your domain gateways.

**Minger verification lookups also trigger Domain Sharing lookups**
When this option is enabled and Minger is used by any of your gateways for address verification, in addition to querying the Minger host designated on the Verification screen[461], MDaemon will also query your Domain Sharing[64] hosts. This is a global option, applying to all gateways set to use Minger for address verification.

## Access

**Honor dequeue requests from these IPs**
Select this switch and MDaemon will honor ETRN/ATRN requests made from any IP listed in the associated address list.

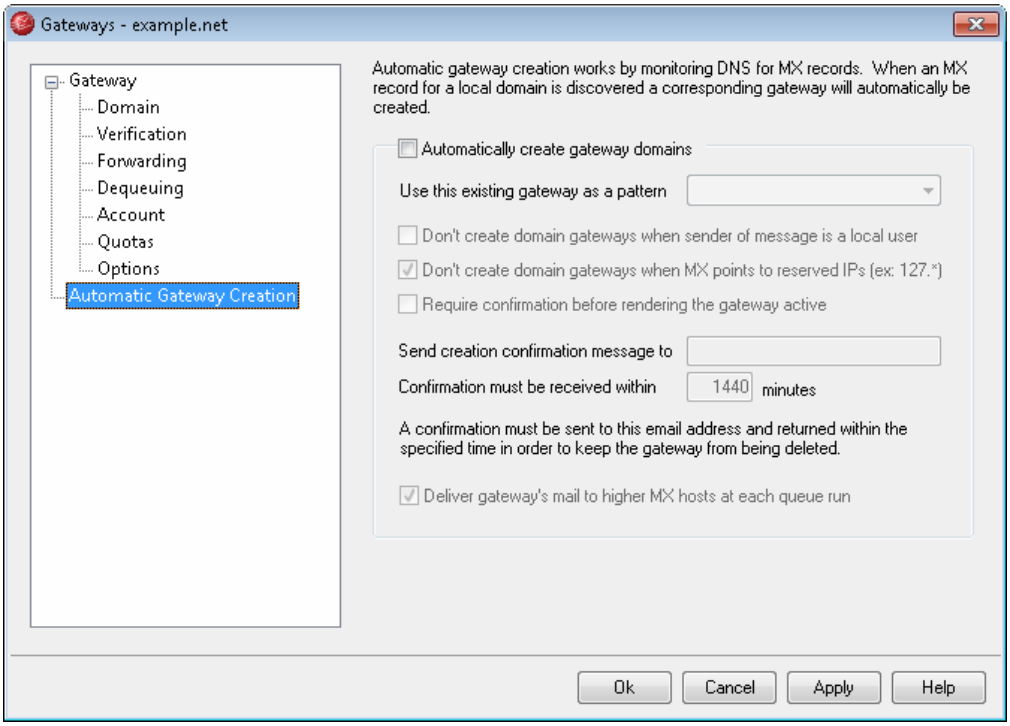
**Ignore dequeue requests from these IPs**
Select this switch and MDaemon will ignore ETRN/ATRN requests that are made from any IP listed in the associated address list.

**Add new IP**
To add a New IP to the current list simply enter the IP into this text box and click the *Add* button.

**Remove**
Click this button to remove a selected entry from the list of IP addresses.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 8.1.2 Automatic Gateway Creation




**Automatic Gateway Creation (MDaemon PRO only)**

This feature is used to automatically create a Domain Gateway 458 for a previously unknown domain when another source attempts to deliver that domain's messages to MDaemon, and a DNS query lists MDaemon's location as a valid MX record.

For example:

With automatic gateway creation enabled, if MDaemon's Default Domain IP address is `192.0.2.0` and a message is delivered via SMTP for an unknown domain `example.com`, MDaemon will perform MX and A-record queries on `example.com` to see if `192.0.2.0` is a known mail relay host for it. If the results of the DNS queries state that MDaemon's IP address is a valid MX host for `example.com` then MDaemon will automatically create a new Domain Gateway for it and accept its email. Messages for `example.com` will then be stored in a special folder and, if you so choose, spooled to higher level MX hosts at each remote mail processing interval. This feature effectively enables you to become a backup server for another domain by simply configuring the DNS system to use your IP as an alternate MX host.

To help secure this feature, MDaemon can be configured to send a confirmation request to an email address of your choice. While MDaemon is waiting for the confirmation response, messages for the domain will be accepted and stored but not delivered. Confirmation requests must be replied to within an amount of time that you designate or the automatically created gateway will be removed and all stored messages deleted. If confirmation is received before the time has expired then the stored messages will be delivered normally.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

It might be possible for a malicious person or "spammer" to attempt to exploit this feature by configuring their DNS server to list your MDaemon's IP address as one of their MX hosts. Automatic Gateway Creation must therefore be used with caution. To aid in preventing possible exploitation we recommend utilizing the *Send creation confirmation message to...* feature whenever possible.

**Automatically create gateway domains**
Click this checkbox if you want MDaemon to automatically create Domain Gateways based upon the results of DNS queries.

**Use this existing gateway as a pattern**
Choose a Domain Gateway from this drop-down list and MDaemon will use its settings as a template for all future automatically created gateways.

**Don't create domain gateways when sender of message is a local user**
Enable this control if you do not want messages originating from local users to trigger automatic gateway creation.

**Don't create domain gateways when MX points to reserved IPs**
Click this check box if you wish to prevent an automatic gateway creation when the MX record points to a reserved IP address such as 127.*, 192.*, or the like.

**Require confirmation before rendering the gateway active**
When this control is enabled, MDaemon will send a confirmation message to the email address of your choice in order to determine whether the automatically created gateway is valid. MDaemon will continue to accept messages for the domain in question but will not deliver them until confirmation is received.

**Send creation confirmation message to**
Use this text box to designate the email address to which confirmation messages will be sent.

**Confirmation must be received within XX minutes**
This control is for designating the number of minutes that MDaemon will wait for a response to any given confirmation message. If this time limit expires then the Domain Gateway in question will be deleted.

**Deliver gateway's mail to higher MX hosts at each queue run**
If you want MDaemon to attempt to deliver this gateway's messages to higher level MX hosts each time that the remote queue is processed then enable this control.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**See:**

**Domain Gateways** 458
**Gateway Editor** 459

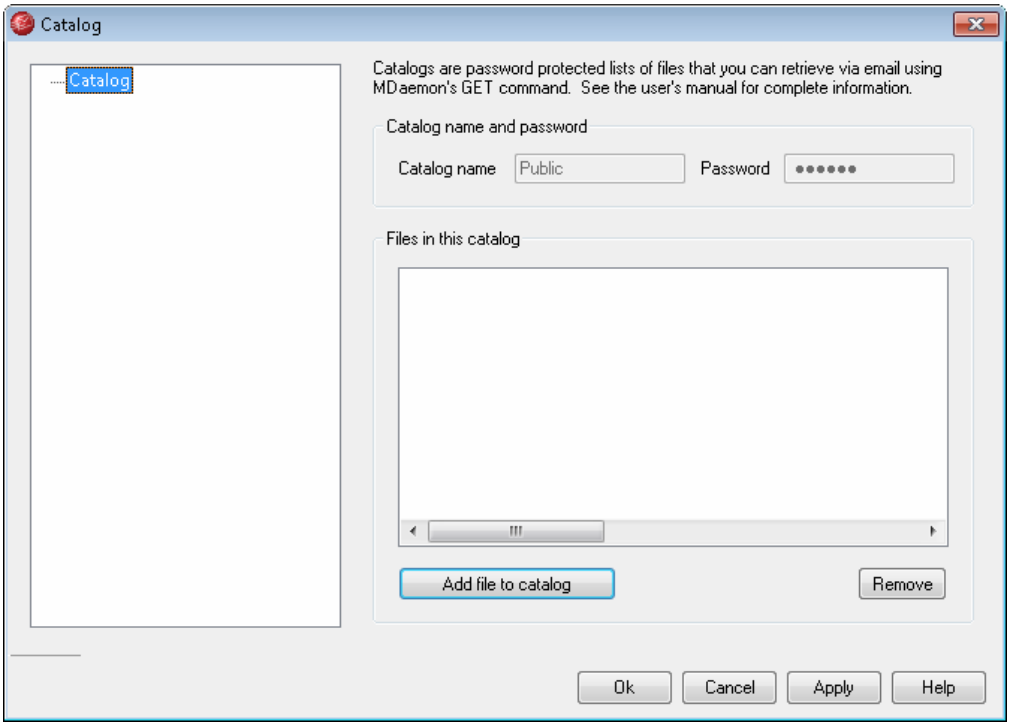
*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Section

# 9 Catalogs Menu

## 9.1 Catalog Editor




Use the Catalogs » New Catalog... or Catalogs » Edit Catalog... menu selection to open the Catalogs Editor for creating or editing a file catalog. Catalogs give users the ability to request files across the network and have them encoded and mailed back to them. Catalogs work by allowing the mail administrator to assign a "magic name" (i.e. shortcut) to files on disk. Magic names are like aliases which point to a specific file located somewhere accessible to MDaemon. A user can then use a special type of email message to request the file using the magic name. The format of this email message is described in the Remote Server Control 504 section (see the **GET** command in Mailing List and Catalog Control 506.

### Catalog name and password

**Catalog name**
Use this field to enter a name for the file catalog.

**Password**
Use this field to enter a password for the file catalog.

Passwords are not required for all catalogs. You may choose to make catalogs accessible without a password.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

Mailing List and Catalog Control 506

**File in this catalog**

This window displays all the files and their associated "magic names" currently registered as members of the specified catalog. Double click on an entry in this window to remove it from the catalog.

**Remove**
Click this button to remove a selected entry from the list of files.

**Add file to catalog**
Click this button if you wish to add a file to the catalog. After choosing the file that you wish to add, you will be prompted for the *Magic name* that you wish to assign to the file. Click Ok and the file and magic name will be added to the list.

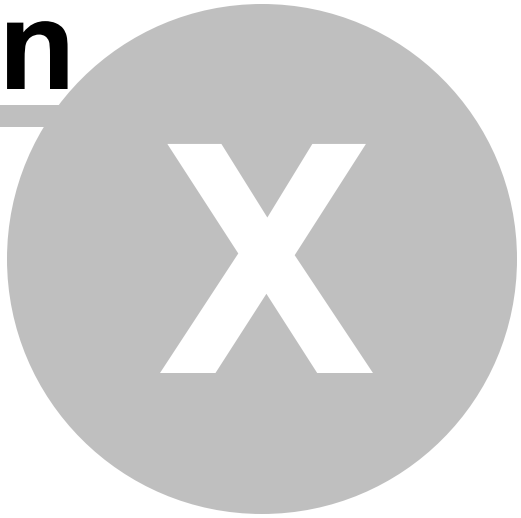
## The PUBLIC Catalog

The PUBLIC catalog is an exception to the normal rules governing access to file catalogs. Typically, to access a catalog requires a password that has been assigned to the catalog. With the PUBLIC catalog the password is not required. Files listed in the PUBLIC catalog are available to anyone who knows the file's magic name.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

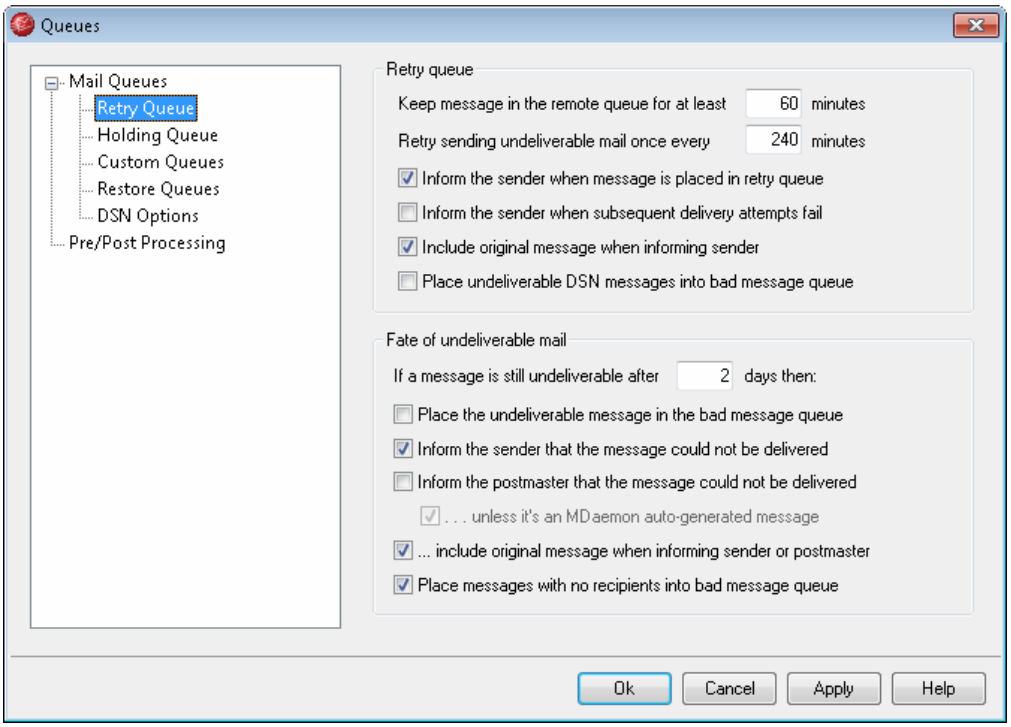
# Section



# 10 Queues Menu

## 10.1 Mail Queues

### 10.1.1 Retry Queue




The Retry Queue dialog, located under Queues » Mail Queues, is used to determine how MDaemon will handle messages that cannot be delivered due to some non-fatal error, such as when the receiving server is temporarily unavailable.

**Retry Queue**

**Keep message in the remote queue for at least XX minutes**
This setting governs the length of time a message will remain in the remote queue before being removed and placed in the retry queue. The remote queue will generally attempt to deliver the message more frequently than the retry queue.

**Retry sending undeliverable mail once every xx minutes**
This setting determines how frequently the messages in the retry queue are processed.

**Inform the sender when message is placed in retry queue**
When this box is checked, MDaemon will inform the sender when his or her message is removed and placed in the retry queue. The text of this message can be found (and edited) in the `DeliveryWarning.dat` file in MDaemon's `\app\` folder.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Inform the sender when subsequent delivery attempts fail**
If a delivery attempt of a message in the retry queue fails, a message explaining this fact will be dispatched to the sender of the message. The text of this message can be found (and edited) in the `DeliveryWarning.dat` file in MDaemon's `\app\` folder.

**Include original message when informing sender**
Click this option to include the original message as an attachment in the above notification messages to the sender.

**Place undeliverable DSN messages into bad message queue**
Click this checkbox if you wish to place undeliverable Delivery Status Notification (DSN) messages into the bad message queue rather than retrying them.

This only applies to DSN messages generated by MDaemon.

## Fate of Undeliverable Mail

**If a message is still undeliverable after xx days then:**
This setting determines the number of days that a message can remain in the retry queue before being removed. If you enter "0" days into this option then the message will be bounced back after the first retry attempt. The default setting is 2 days.

**Place the undeliverable message in the bad message queue**
When this option is enabled, a message will be moved to the bad message queue once it has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option.

**Inform the sender that the message could not be delivered**
Once a message has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option, this switch will cause MDaemon to send a message to the sender informing him that the message has been permanently removed from the server. The text of this message can be found (and edited) in the `DeliveryError.dat` file.

**Inform the postmaster that the message could not be delivered**
If this switch is enabled, the postmaster will be notified when a message has been permanently removed from the retry system.

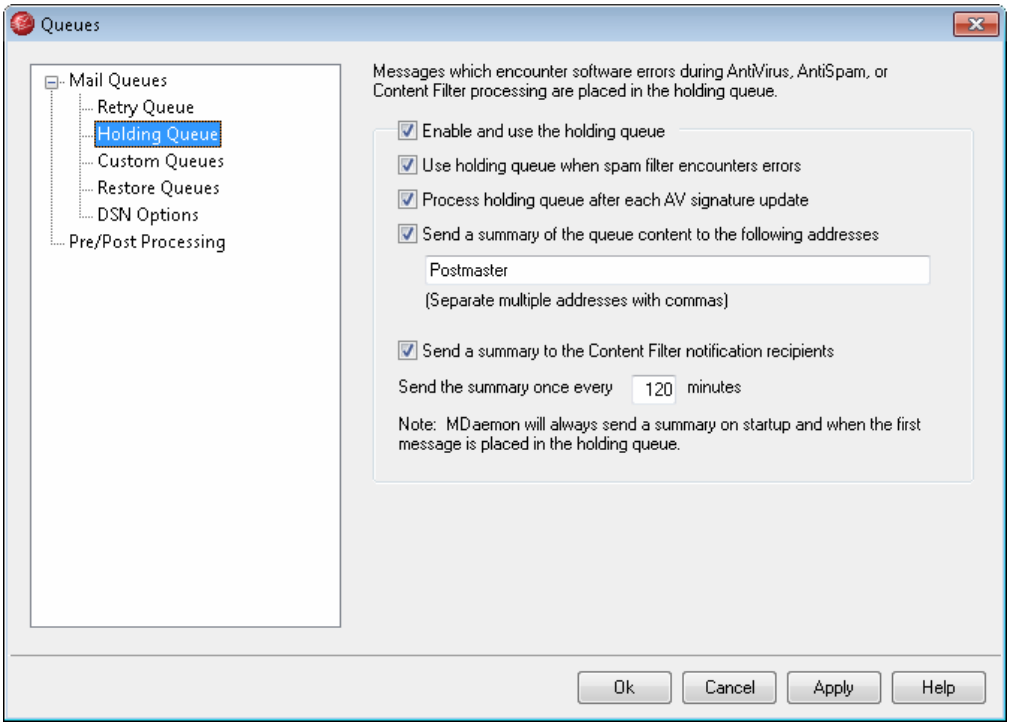
**. . . unless it's an MDaemon auto-generated message**
By default, the retry system will not inform the postmaster that a message could not be delivered when that message was auto-generated by MDaemon. Clear this checkbox if you wish to inform the postmaster about the failure of those messages as well. Examples of auto-generated messages are return-receipt notifications, Autoresponder generated messages, results of account processing, and so on.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**...include original message when informing sender or postmaster**
Click this option to include the original message as an attachment in the delivery failure messages to the sender or postmaster.

**Place messages with no recipients into bad message queue**
When this option is enabled, messages with no recipient data will be moved to the bad message queue. When disabled, they will be deleted. This option is enabled by default.

### 10.1.2 Holding Queue




The Holding Queue, located under Queues » Mail Queues can be used to receive messages that cause software exceptions during AntiVirus, AntiSpam, or Content Filter processing. If a software error occurs when processing a message it will be moved into the holding queue and not delivered.

Messages placed into the holding queue will stay there until the administrator takes some action to remove them. There is a *Process Holding Queue* button on MDaemon's toolbar and an identical option on the Queues menu bar. You can also process the messages by right-clicking the holding queue on the main interface and then selecting "Re-Queue" from the right-click menu. Processing the holding queue will move all of its messages into either the remote or local queues for normal mail processing. If the error that caused a message to be placed into the holding queue still exists then that message will be placed back into the holding queue when the error reoccurs. If you want to attempt to deliver the holding queue's messages regardless of any error which might occur, then you can do so by right-clicking the holding queue on the main interface and then selecting "Release" from the right-click menu. When releasing messages from the holding queue a confirmation box will open to remind you that the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

messages could contain viruses or otherwise not be able to filter properly through the Content Filter, AntiSpam and/or AntiVirus engines.

### Holding Queue

**Enable and use the holding queue**
Click this check box to activate the holding queue. Messages that cause software exceptions during AntiVirus and Content Filter processing will be moved to this queue whenever an error occurs.

**Use holding queue when spam filter encounters errors**
Click this option if you wish to move messages that cause errors during Spam Filter processing to the holding queue.

**Process holding queue after each AV signature update**
When this option is enabled, the holding queue will be processed automatically each time after the SecurityPlus for MDaemon 210 virus signatures are updated.

**Send a summary of the queue content to the following addresses**
If you wish to send a summary of messages contained in the holding queue to one or more email addresses at regular intervals then click this option and list the addresses in the text space provided. When listing multiple addresses, separate them with commas.

Notification messages are sent at MDaemon startup, the first time a message is placed into the holding queue, and at the interval specified in the *Send the summary once every XX minutes* option below.

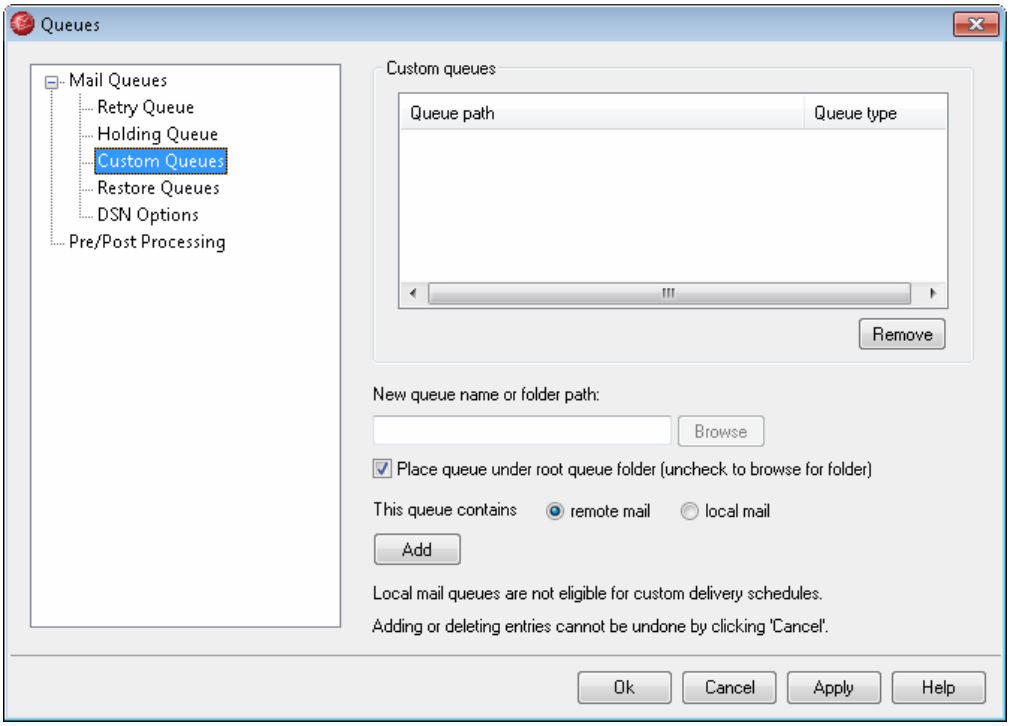
If a notification message causes a software error then it may not be delivered to remote recipients. It will, however, still be delivered to local recipients.

**Send a summary to the Content Filter notification recipients**
Click this option if you want an additional copy of each notification message to be sent to the Content Filter's designated notification Recipients 227.

**Send the summary once every XX minutes**
Use this option to designate the number of minutes that will pass before MDaemon will send a holding queue notification message to each specified address or Content Filter recipients.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

### 10.1.3 Custom Queues




Use the Custom Queues dialog under Queues » Mail Queues to create custom local and remote mail queues. Custom queue support makes it possible for you to have MDaemon monitor several locations from which to send mail. You can create new queues and designate them as local or remote, and you can then use Content Filter rules to cause messages to be automatically placed into your custom mail queues, and for remote queues you can use the Event Scheduler[145] to create custom schedules to control how often those queues will be processed.

#### Custom Queues

This area displays an entry for each custom queue, listing its file path and whether it is local or remote.

**Remove**
If you wish to remove a queue from the list, select its entry and then click the *Remove* button.

When you delete a custom queue, any custom schedules or content filter rules associated with that queue will also be deleted.

**New queue name or folder path**
Use this text field to specify the queue name or path to the folder that you wish to designate as a mail queue. If you wish to enter a full file path or browse to a specific folder, then clear the *"Place queue under root queue folder (uncheck to browse for*

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*folder)*" option below. If you do not clear that option then the queue will be created under MDaemon's `\queues\` folder.

**Place queue under root queue folder (uncheck to browse for folder)**
If this check box is enabled, the queue name specified in the "*New queue name or folder path*" option will be created as a subfolder under MDaemon's `\queues\` folder. If you disable this check box, the queue name specified will be created as a subfolder under MDaemon's `\app\` folder. When this option is disabled you can also type a full file path or use the Browse button to navigate manually to the folder you wish to use as a custom queue.

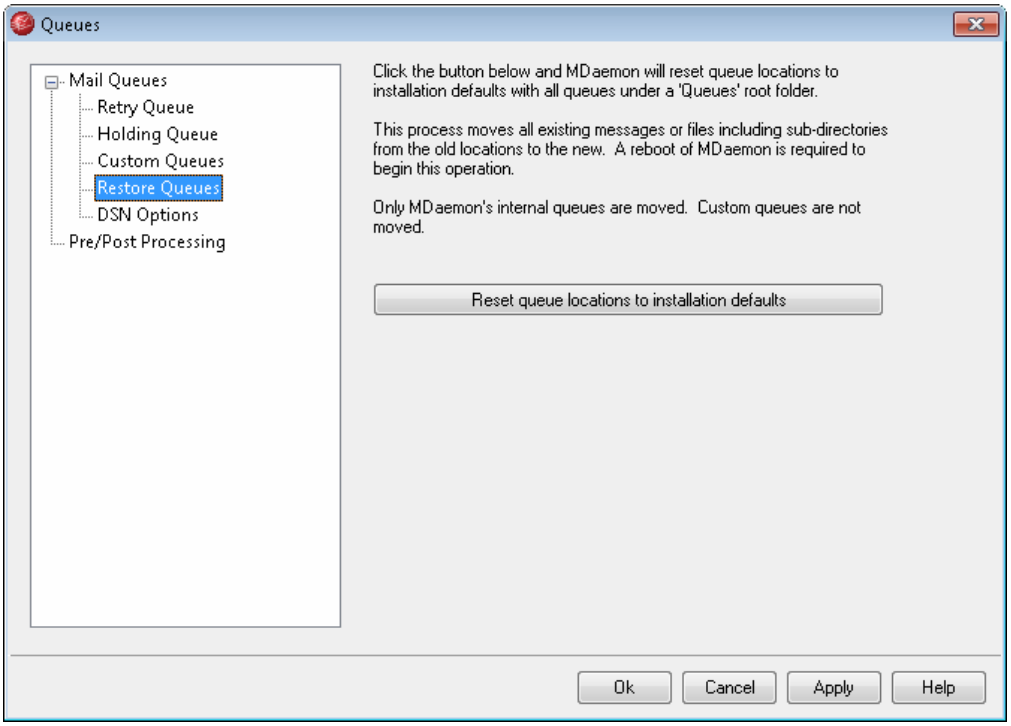
**This queue contains...**

**...remote mail**
Choose this option if you want the custom mail queue to be used for remote mail.

**...local mail**
Choose this option if you want the custom mail queue to be used for local mail.

**Add**
After you have chosen the name, location, and type for your queue, click the *Add* button to add it to the list of custom queues.

### 10.1.4 Restore Queues

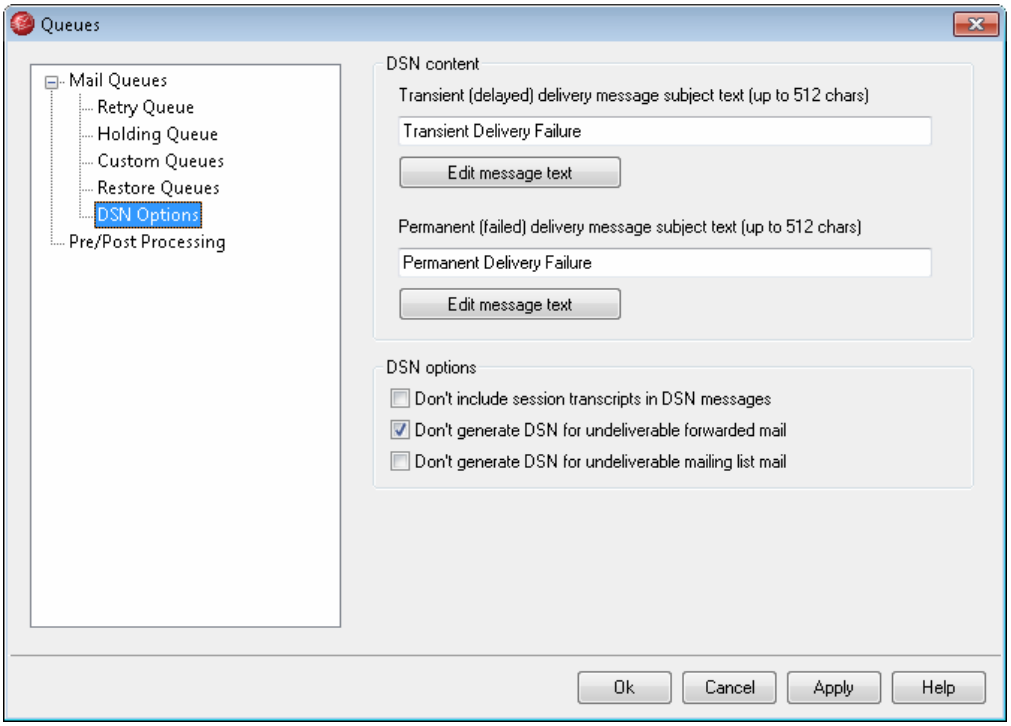



Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**Reset queue locations to installation defaults**
By default, a new installation of MDaemon stores message queues such as Remote, Local, Raw, and the like under the \MDaemon\Queues\ subfolder. Previous versions of MDaemon stored queues elsewhere. If your installation of MDaemon is using the old folder locations and you would like to move your queues to this more organized structure then click this button and all queues and the files and messages they contain will be moved for you. After clicking this button you will need to restart MDaemon for the changes to be implemented.

Custom Queues 486 will not be moved by this feature.

## 10.1.5 DSN Options




When MDaemon has a problem delivering a message, whether it is a temporary or permanent delivery failure, a Delivery Status Notification (DSN) message is sent to the sender of the message. This screen contains various options related to those DSN messages. It is located at: Queues » Mail Queues/DSN... » DSN Options.

### DSN Content

**Transient (delayed) delivery message subject (up to 512 chars)**
This is the subject heading of the DSN message that will be sent when there is a transient problem causing a delay in message delivery. For example, if the recipient's

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

mail server isn't available when MDaemon tries to deliver a message, MDaemon will continue trying to send it at designated intervals, and it will send this DSN message informing the sender of the problem.

**Edit message text**
Click this button to edit the text that is inserted into the body of the transient delivery DSN message.

**Permanent (failed) delivery message subject text (up to 512 chars)**
This is the subject heading of the DSN message that will be sent when there is a problem that makes it impossible for MDaemon to deliver a message. For example, if the receiving mail server rejects the message, stating that the recipient's email address doesn't exist, MDaemon will stop trying to deliver the message and will send a DSN message informing the sender that the message cannot be delivered.

**Edit message text**
Click this button to edit the text that is inserted into the body of the permanent, or failed delivery DSN message.

### DSN Options

**Don't include session transcripts in DSN messages**
Click this option if you do not wish to include SMTP session transcripts in delivery error and warning messages. This option is disabled by default.

**Don't generate DSN for undeliverable forwarded mail**
When this option is enabled, forwarded messages that encounter permanent, fatal delivery errors or expire from the Retry queue 482 will be moved to the bad messages queue, with no DSN messages being sent to the original sender. This option is enabled by default.

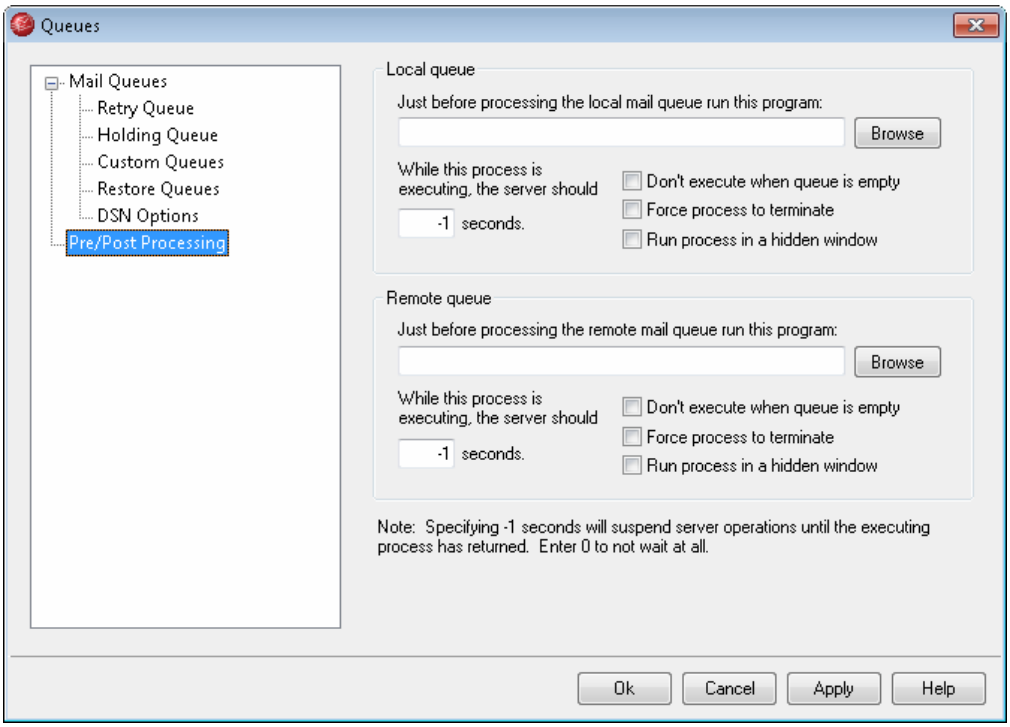
**Don't generate DSN for undeliverable mailing list mail**
When this option is enabled, mailing list messages that encounter permanent, fatal delivery errors or expire from the Retry queue will be deleted, with no DSN messages being generated. When this option is disabled, a DSN message will be sent to the list's designated *SMTP 'Bounce' address* 444. This option is disabled by default.

**See:**

**Retry Queue** 482

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

## 10.2 Pre/Post Processing




### Local and Remote Queue Pre/Post Processing

**Just before processing the (local/remote) mail queue run this program**
This field specifies a program path and name that will be executed just prior to the processing and delivery of any RFC-2822 messages that might be in the local or remote message queues. If complete path information is not provided, MDaemon will first search for the executable in the MDaemon directory, then in the Windows System directory, next in the Windows directory, and finally the directories listed in the PATH environment variable.

**...suspend all operations for xx seconds**
The value entered here determines how MDaemon will behave while the specified program is in progress. MDaemon can be configured to pause its execution thread for the number of seconds specified while waiting for the process thread to return. If the process returns before the number of seconds has elapsed, MDaemon will resume its execution thread immediately. If you enter "0" in this option MDaemon will not suspend operations at all. Entering "-1" will cause MDaemon to wait until the process returns, no matter how long that might be.

**Don't execute when queue is empty**
Enable this switch if you do not want the specified program to run when the queue is empty.

**Force process to terminate**
Sometimes the process you need to run may not terminate on its own. This switch will cause MDaemon to force the session to terminate once the time specified in ...

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

*Suspend all operations for XX seconds* has elapsed. This switch does not work if the elapsed time interval is set to "-1".

**Run process in a hidden window**
Click this checkbox if you want the process to run in a hidden window.

## 10.3 Queue and Statistics Manager

MDaemon's Queue and Statistics Manager is accessed from within MDaemon under the Queues » Queue and Statistics Manager menu selection. The Queue and Statistics Manager is made up of a four-page dialog. Each of these pages has been designed to serve a distinct and specific purpose while also maintaining a simple format that makes them very easy to use.

### Queue Page 492

The default tab is the *Queue Page*. From this page you can easily manage all of MDaemon's standard mail queues, as well as the User Account mailbox folders. By simply clicking on the queue or user of your choice, a list of all message files contained within the specified queue will be displayed along with several key pieces of pertinent information about each message: the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location. In addition, controls are provided that make it easy to copy or move messages between folders, or delete them completely.

### User Page 495

The *User Page* displays a list of all MDaemon users. This list includes their full name, mailbox name, the number of messages in their mailbox, the amount of disk space that their account is taking up, and the date that they last checked their mail. This list can also be saved to disk as a text file, or it can be saved in comma delimited format for use with databases.

### Log Page 497

With this dialog you can display MDaemon's *Log Files* in a simple list format. This feature is very useful for quickly examining the history of MDaemon's mail transactions because it condenses the selected *Log File* into a columnar list which contains: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful. You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Logs displayed on the *Log Page* can be saved as a text file or in comma delimited format for use with databases.

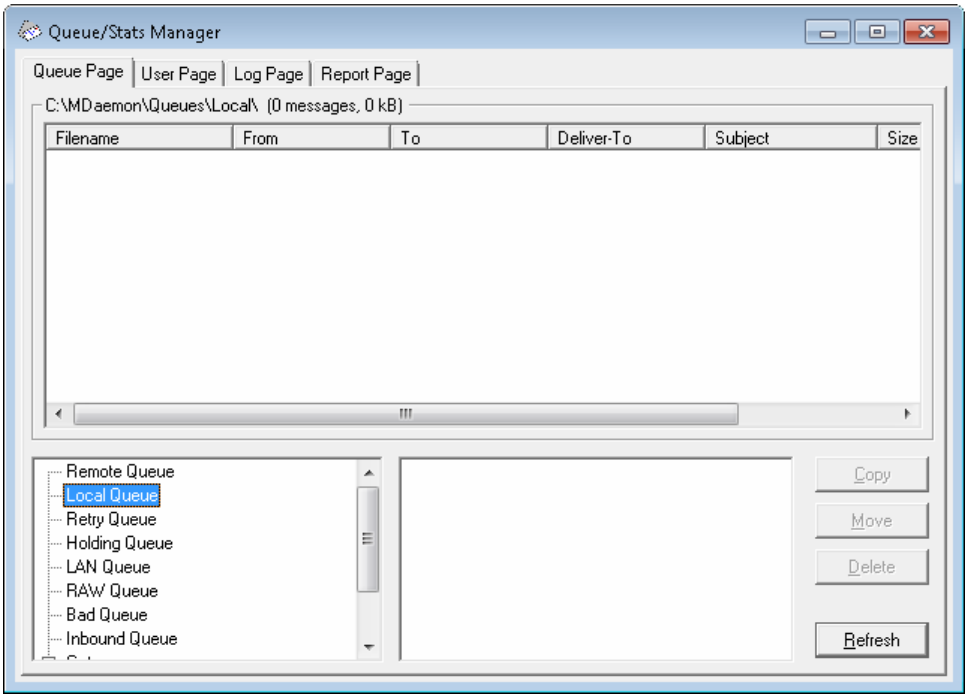
### Report Page 499

The last tab is the *Report Page*. With this feature you can produce a report containing all of MDaemon's configuration settings, written in a plain text readable format.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Because of the large number of optional settings and configurations in MDaemon, this can greatly speed the process of administering configuration changes as well as aid in diagnosing possible configuration problems. Additionally, this report is displayed in a text editable format that makes it possible to Copy/Paste the information it contains (using the right-click shortcut menu), or add notations or other information to the file before saving it.

### 10.3.1 Queue Page




**Queue page list box**

When a queue or user is chosen from the *Message Queues* area or the user list box beside it, a list of all message files contained within the selected queue will be displayed in the main list box on this page. This list contains each message's file name, the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location (listed by date and time).

Above this box the complete file path to the currently displayed directory is given, as well as the number of messages displayed and the size of the directory.

You may copy, move, or delete one or more files by selecting them from the list and then clicking the appropriate button below it.

The content of these files may also be edited directly from the *Queue Page* list box. Simply double-click the file that you wish to edit (or choose "Edit" from the right-click shortcut menu) and the file will be opened in Notepad for editing.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

If you want the Queue and Statistics Manager to open an editor other than Notepad by default, then you must edit the `mdstats.ini` file located in the `\MDaemon\app\` folder. Change the "`Editor=`" key located under the `[QueueOptions]` section heading to `Editor=MyEditor.exe`. If the file path of the `*.exe` file is not in your current path, then you will have to include the path here as part of the file name.

The list box can be navigated by using the vertical or horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *Queue Page* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z, 1-2), or click twice to sort it in descending order (Z-A, 2-1). Columns can also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

### Selecting Files

| | |
|---|---|
| **To select files individually** | Click the desired file. |
| **To select contiguous files** | Click the first file in the contiguous list of files that you wish to select, then while holding down the SHIFT key, click the last contiguous file in the desired list.<br>Alternatively, you may use the ARROW, HOME, END, PAGE UP, and PAGE DOWN keys, while holding down the SHIFT key, to select files in contiguous order. |
| **To select non-contiguous files** | Click on the desired files in the **File Name** column while holding down the CTRL key. |

**Message queues**
Click an in the lower left pane and a list of all files contained within the specified queue will be displayed in the *Queue Page* list box. If you click the *User Folders* option, a list of all MDaemon users will be displayed in the *User List Box* to the right of the *Message Queues* section.

**Users list box**
This box displays a list of all MDaemon users when the *User Folders* option is clicked in the *Message Queues* section (lower left pane). Click a user's name to display a list of all message files currently contained in the user's mailbox folder.

**Refresh**
Because mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them - you should regularly click this button to refresh any list of files that you may have displayed.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

You can edit the MDstats.ini file to cause displayed lists to automatically refresh. To do this simply open the MDstats.ini file located in MDaemon's \app\ directory and edit the AutoRefresh key under the [QueueOptions] heading to reflect the number of seconds that you wish to elapse between refreshes. Entering the value "0" means that you do not want the list to automatically refresh. Example: AutoRefresh=15 (the list would refresh every 15 seconds).

**Copy**
When one or more files are selected, click this button to copy the selected files to another queue or user's mailbox folder. After clicking this button the *Copy Message(s)* dialog box will open, from which you can select the desired location to which you wish to copy the selected files.

**Move**
When one or more files are selected, click this button to move the selected files to another queue or user's mailbox folder. After clicking this button the *Move Message(s)* dialog box will open, from which you can select the desired location to which you wish to move the selected files.

Files copied or moved to other queues will rarely retain their original file names. To avoid overwriting files of the same name that may already be in the queue, MDaemon always calculates the next destination filename based on the HIWATER.MRK file located in the destination folder.

**Delete**
When one or more files are selected in the *Queue Status List Box*, click this button to delete the selected files. After clicking this button a confirmation box will open asking if you really do wish to delete the selected files.

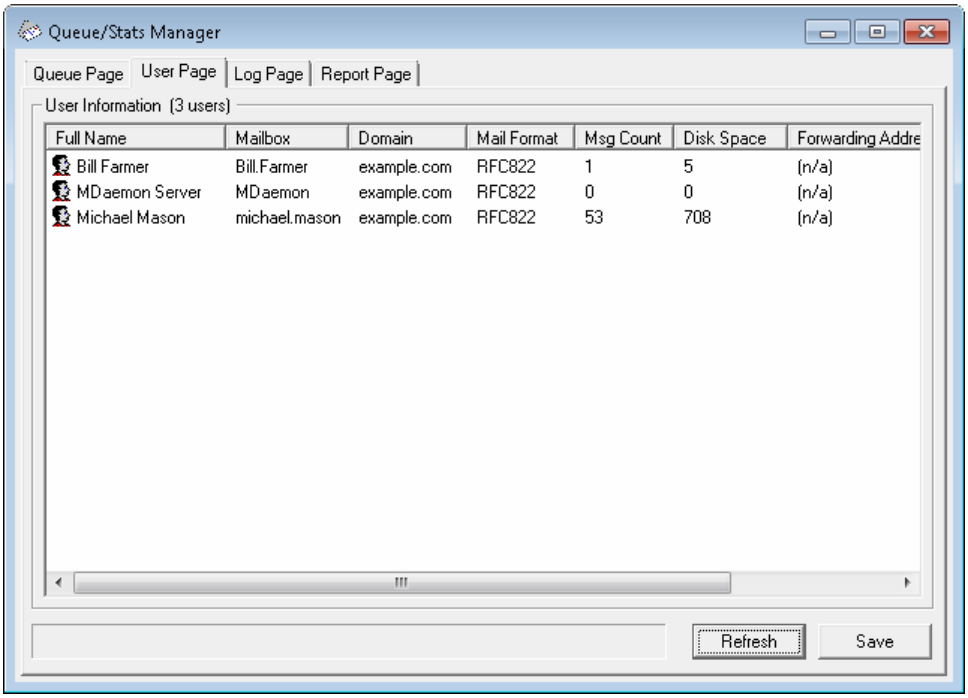
Mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them. For this reason you should be aware that when copying, moving, or deleting files you may at times encounter a message stating that the action that you are attempting cannot be completed. This will occur when the message file that you are attempting to work with has already been removed by MDaemon before the desired action has begun. By clicking the *Refresh* button, you can update the current list of files displayed in the list box.

You can prevent messages from being moved out of the queue while you are editing them by editing the MDstats.ini file. To do this simply open the MDstats.ini file located in MDaemon's

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

> \app\ directory and change the LockOnEdit=No key under the [QueueOptions] heading to LockOnEdit=Yes. This will cause a LCK file to be created whenever you are editing a message, which will prevent it from being moved out of the queue until you are finished with it.

### 10.3.2 User Page




**User information**
When the *User Page* is chosen, a list of all MDaemon accounts is loaded into the *User Information* list box. This list contains each user's full name, the name of their mailbox, the domain to which the account belongs, the number of messages it contains, its mail format, the amount of disk space (in kilobytes) that the account is taking up, their forwarding address, and finally, the date that their mail was last checked. Given that the information contained in this list is constantly changing, it can be easily updated by clicking the *Refresh* button.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *User Information* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z), or click twice to sort it in descending order (Z-A). Columns may also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width. Further, you can double-click any entry and MDStats will be shifted to the *Queue Page* with

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

the contents of their mailbox folder displayed.

By default, the list displays the Message Count not file count, and the Disk Space used *by messages* not the space used by all files in the directory. This is the *Quota* information reported by MDaemon. Alternatively, you can display the *file* count and disk space used by all *files* instead of by messages. To change this setting simply open the `MDstats.ini` file located in MDaemon's `\app\` directory and change the `ShowQuota=Yes` key under the `[UserOptions]` heading to `ShowQuota=No`.

User folders contain a file called "`hiwater.mrk`" which is used to determine some of this user information. You should avoid deleting this file unnecessarily as it will prevent the Queue and Statistics Manager from being able to obtain some of the information listed in the *User Information* list box.

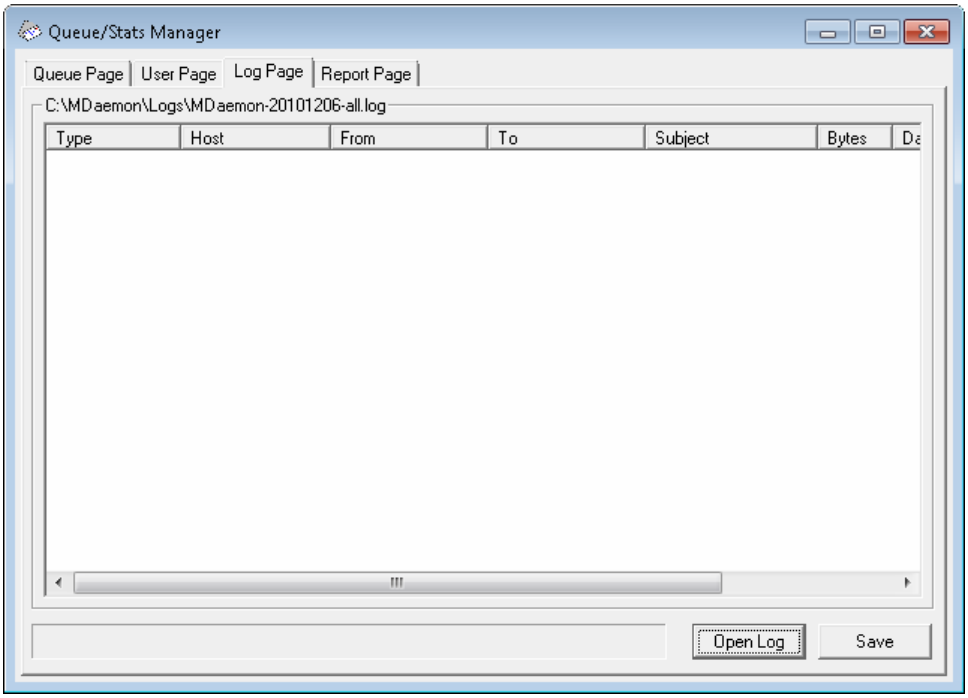
**Refresh**
User statistics such as the number of messages contained in their mailboxes, and the amount of disk space that their accounts are using, are constantly changing. You can easily update the information contained in the *User Information* list box by clicking the *Refresh* button. This will immediately make all displayed information current.

**Progress indicator**
Because *User Information* lists can at times be very large, below the *User Information* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded.

**Save**
The information contained in the *User Information* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 10.3.3 Log Page




**Log report**
The *Log Report* list box displays MDaemon's detailed log files that you select through the *Open Log* button and the Windows Open dialog that follows it. The *Log Report* display provides a quick and easy way to review the history of mail transactions that MDaemon has processed without having to sort through the large volume of information that MDaemon log files may sometimes contain. When a *Log Report* is displayed in this list box the Queue and Statistics Manager breaks it down into a simple format containing: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful.

You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Using the right-click shortcut menu you can copy/paste this detailed log portion to a text editor for saving or editing should you desire to do so.

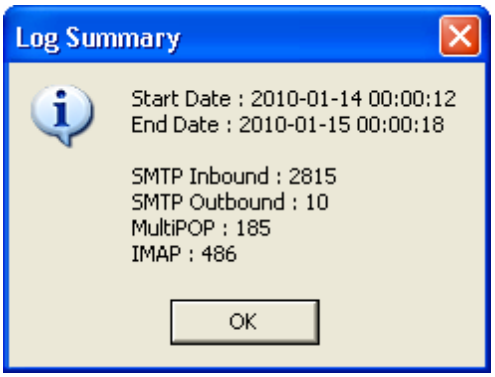
The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can resize the list box's columns by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

The *Log Page* will display log files that have been compiled using either the *Log detailed mail sessions* or the *Log summarized mail sessions* option located under Logging » Log Mode. However, we highly recommend that you use the *Log detailed mail sessions* option. When using the *Log summarized mail sessions* format you will find that there is very little information that will be displayed in your *Log Report*. Because the *Log Page* itself condenses the detailed log into a summary view of MDaemon's activity, while still providing the ability to look at the detailed view of every transaction when necessary (by double-clicking an entry), there is no need to have MDaemon summarize the log file while compiling it.

**Open log**
Click this button to open the Windows Open dialog for choosing which log file that you wish to view. If you click this button when there is a *Log File* already displayed in the *Log Report* list box, you will be given the option to append the new file to the one that is already displayed.

After a log is displayed, a message box will be opened which contains a summary of the selected log. When saving a Log Report as a text file, this log summary will be appended to it.

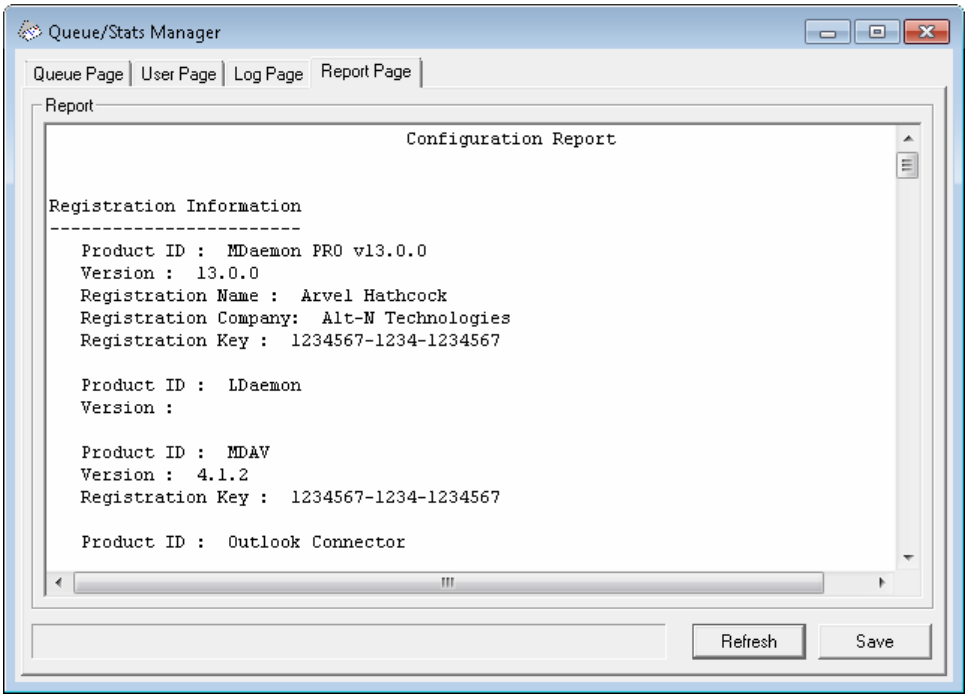



**Progress indicator**
Because *Log Files* can be very large, below the *Log Report* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded or saved.

**Save**
The information contained in the *Log Report* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

### 10.3.4 Report Page




**Report**
When the *Report Page* is clicked, a comprehensive report will be produced that lists every setting within MDaemon in an easily readable text format. This feature greatly decreases the amount of time needed by an administrator to check MDaemon's many configuration settings, and it can aid in quickly solving possible configuration problems.

You can navigate through this report using either the scroll bars or the CURSOR keys, and the *Report* display is also a text editor - making it possible to insert notations or additional information that you may want on the report before saving it to a file. Additionally, you can use the shortcut menu to Cut, Copy, and Paste, to and from this display by right-clicking your mouse and making the desired selection from the menu that opens.

**Refresh**
Click this button to update the currently displayed *Report* of MDaemon settings.

**Progress indicator**
As with the other tabs in the Queue and Statistics Manager, the *Report Page* contains a progress indicator bar that serves as a visible indicator that the program is still operating while large files are being loaded or saved.

**Save**
Click this button to save the currently displayed *Report*. After clicking this button a standard Save As dialog will open so that you can designate a file name and location where you want to save it.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

## 10.3.5 Customizing the Queue and Statistic Manager

### 10.3.5.1 MDstats.ini File

**Customizing the Queue/Statistic Manager**

The following is a list of settings that can be modified in the `MDstats.ini` file located in MDaemon's `\app\` directory:

**[MDaemon]**

| | |
|---|---|
| AppDir=C:\mdaemon\app\ | Location of MDaemon's \app\ directory. |

**[QueueOptions]**

| | |
|---|---|
| Editor=NOTEPAD.EXE | Editor to use when a message is double-clicked, or when a message is right-clicked and then Edit is selected. |
| LockOnEdit=No | Whether or not to create a LCK file when editing a message. This will prevent a message from being moved out of the queue while it is being edited. |
| AutoRefresh=Yes | Time (in seconds) between auto refreshes of the message listing. 0 means no auto refresh. |
| ShowDirectories=Yes | Show subdirectories of the queues in the list box in addition to the messages. Directories will appear as <DirectoryName>. |

**[UserOptions]**

| | |
|---|---|
| ShowQuota=Yes | Determines whether the user listing displays quota information (message count and disk space just like MDaemon calculates it) or file information (number of files and total disk space). |

**[LogOptions]**

| | |
|---|---|
| ShowUnknown=Yes | Show sessions that MDStats couldn't determine if they were inbound or outbound, SMTP or POP. |
| ShowSmtpInbound=Yes | Show SMTP inbound sessions. |
| ShowPopInbound=Yes | Show POP inbound sessions (mail checks). |
| ShowSmtpOutbound=Yes | Show SMTP outbound sessions. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| ShowPopOutbound=Yes | Show POP outbound sessions (MultiPOP, DomainPOP). |
| ShowRFC822=Yes | Show RFC822 local mail deliveries. |
| ShowSmtpHelo=Yes | For SMTP inbound sessions, show HELO domain in the Host column. |
| IgnoreEmptyPop=Yes | Ignore mail checks when no mail was deliverd. |
| ShowImap=Yes | Shows IMAP Sessions. |
| **[Remap]** | Drive letter remapping; for running MDStats from a different machine than the one MDaemon is on. |
| C:=\\server\c | When reading from MDaemon.ini, replace "C:" with "\\server\c". |
| **[Special]** | |
| OnlyOneInstance=No | Allow only one instance of MDStats to run. Attempting to open it again will activate the instance that is already running. |

**See:**

**MDStats Command Line Parameters** 501

### 10.3.5.2 MDStats Command Line Parameters

**Note:** All command line parameters are not case sensitive.

| | |
|---|---|
| Number 1 through 8 | Display a specified queue in the Queue Page. |
| | = Remote Queue |
| | = Local Queue |
| | = Retry Queue |
| | = LAN Queue |
| | = RAW Queue |
| | = Bad Queue |
| | = SmtpIn Queue |
| | = Save Queue |

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

| | |
|---|---|
| /L[N] [InputFile] [OutputFile] | Produce a log file report. Specifying an "N" after the "L" means do not save as a comma delimited file. |
| /A | If producing a log file report, append new information to the output file rather than overwriting it. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# Section

# 11 Additional MDaemon Features

## 11.1 MDaemon and Text Files

MDaemon uses a number of plain text files to store some of its data, system generated message templates, and configuration settings, which provides a great deal of flexibility. You can create new text files from within MDaemon by using the File » New menu selection. This can be useful for quickly creating data files for use with Autoresponders and various other MDaemon features, such as RAW files.

### Editing MDaemon Files

MDaemon's various data files are plain text and can be edited in Notepad. You can easily open any of these files from within MDaemon by using the File » Open » Empty Text File menu selection. By default this looks in MDaemon's `\app\` folder for `*.txt` files. Switch the *Files of type:* drop down list to "All files" to see the rest of the files contained in that folder.

## 11.2 Remote Server Control via Email

Many functions of MDaemon can be accessed remotely using the email transport system itself. For example, users can gain access to various aspects of their accounts and change or reconfigure them by sending email messages to the server. MDaemon maintains an account for its own use in the user base. This account is reached by sending mail to the mailbox, "`MDaemon@<MDaemon's Domain>`". Messages sent to the server are stored in the server's message directory just like any other user. At queue run time the server will cycle through all the mail it has received and parse each message for special instructions.

Some of these control messages require a valid account on the server, and are password protected. For those commands which require a valid account, the message must be authenticated during the SMTP process using SMTP AUTH.

There are three, broad categories of commands that can be used in email messages: Account Access and Control 504, Mailing List and Catalog 506, and General Email 509.

**See:**

**Account Access and Control** 504
**Mailing List and Catalog Control** 506
**General Email Controls** 509

### 11.2.1 Account Access and Control

The following section lists the account access and control commands available to account holders. All of these commands require the message to be authenticated using

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

SMTP AUTH. Parameters contained in [brackets] are optional. For example: "`name [address]`" could be entered as "Michael" alone or with the optional parameter added: "Michael `user1@example.com`". For more on using the following commands in email messages, see: Remote Server Control via Email 504.

| COMMAND | PARMS | DESCRIPTION |
|---|---|---|
| `ACCOUNT INFO` | none | The status of the account passed in the subject line is mailed back to the originator.<br>Example: `ACCOUNT INFO` |
| `PASSWORD` | new password | The password of the account passed in the subject line will be changed to the one specified.<br>Example: `PASSWORD 32!Mike` |
| `BEGIN SIGNATURE` | none | Begins recording of a new signature file to be appended to messages generated by the account passed in the subject line. Subsequent lines will be treated as the text of the signature file until the word END is encountered on a line by itself or the end of the control message is reached.<br><br>NOTE: The signature file feature is only available for RAW format messages. RFC-2822 mail that arrives at the server using SMTP or POP will not append the signature file. In these cases see your mail client's documentation for information concerning signature files. |
| `BEGIN AUTORESPONDER` | none | Begins recording of a new autoresponder file. Subsequent lines will be treated as the text of the autoresponder until the word END is encountered on a line by itself or the end of the control message is reached.<br><br>Example:<br><br>`BEGIN AUTORESPONDER`<br><br>`I'm on vacation right now. I'll get back to you ASAP.`<br><br>`END`<br><br>To erase an active autoresponder use the same command but without any response text.<br><br>Example:<br><br>`BEGIN AUTORESPONDER`<br><br>`END` |
| `FORWARD TO` | address | The forwarding address for the account passed in the subject line will be changed to [address] and |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | | |
|---|---|---|
| | | mail forwarding will be activated for the account.<br>Ex: `FORWARD TO vacationing@example.com` |
| `UNFORWARD` | none | Mail forwarding will be deactivated for the account specified in the subject line.<br>Ex: `UNFORWARD` |
| `MULTIPOP` | on/off | MultiPOP will be enabled/disabled for the account specified in the subject line.<br>Ex: `MULTIPOP ON`<br>Ex: `MULTIPOP OFF` |

**See:**

**Remote Server Control via Email** 504
**Mailing List and Catalog Control** 506
**General Email Controls** 509

## 11.2.2 Mailing List and Catalog Control

None of these commands require an account on the server; thus the subject line need not contain any special value when specifying these instructions. Parameters contained in [brackets] are optional. For example: "`name [address]`" could be entered as "Michael" alone or with the optional parameter added: "Michael `user1@example.com` ". For more on using the following commands in email messages, see: Remote Server Control via Email 504.

| COMMANDS | PARMS | DESCRIPTIONS |
|---|---|---|
| `SUBSCRIBE` | listname [address] [{real name}] [(pass)] | The originator is added to the membership of the specified list provided that list exists and allows remote subscriptions. If an optional address is specified after the list name then that address is added to the list's membership rather than the address found in the FROM: field of the subscription message. A real name can be added for the subscriber by including it in braces (e.g. {Bill F}. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's subscribe function is switched off.<br>Examples:<br>`SUBSCRIBE mdsupp` |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

```
SUBSCRIBE mdsupp me@example.com {Bill
F}
SUBSCRIBE mdsupp you@example.org
(PASS)
```

| | | |
|---|---|---|
| UNSUBSCRIBE<br>Or<br>SIGNOFF | listname [address] [(pass)] | The originator is removed from the membership of the specified list provided that list exists and contains the originator as a current member. If an optional address is specified after the list's name then that address is removed from the list's membership rather than the address found in the FROM: field of the unsubscribe message. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's unsubscribe function is switched off.<br>Examples:<br>`UNSUBSCRIBE MDSUPP (MDSPASS)`<br>`SIGNOFF MDSupportList me@example.com` |
| DIGEST | listname [address] | The sender is set to receive mail from the list in digest format. If an optional address is specified after the list name then that address is set to digest mode.<br>Examples:<br>`SET DIGEST MDSupportList`<br>`SET DIGEST mdsupp user1@example.com` |
| NORMAL | listname [address] | The sender is set to receive mail from "list" in normal (non-digest) format. If an optional address is specified after the list name then that address is set to receive in normal format instead of the sender.<br>Examples:<br>`NORMAL MDSupportList@example.com`<br>`NORMAL mdsupp@example.com user1@altn.com` |
| NOMAIL | listname [address] | This command sets 'address' to nomail mode. The account will enter a suspended state and will no longer receive list traffic. If no address is specified then the originator of the message will be used.<br>Example:<br>`NOMAIL list@example.com me@example.com` |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | | |
|---|---|---|
| MAIL | listname [address] | This command returns 'address' to normal mode from nomail mode. If no address is specified then the originator of the message will be used.<br>Examples:<br>`MAIL list@example.com`<br>`MAIL list@example.com me@example.com` |
| REALNAME | listname [address] {real name} | This command sets the real name value for "address" who is a member of list "listname" to the given value. The real name must be enclosed in { and } characters.<br>Example:<br>`REALNAME mdsupp@altn.com {Bill Farmer}` |
| GET | catalog magic-name (password) | Retrieves a file from the specified catalog, MIME encodes it in an email message, and sends that message to the originating account or to the one specified in a RESULTS TO directive.<br>Example:<br>`GET utils myutil (mypass)`<br>**NOTE**: The special PUBLIC catalog doesn't require a catalog name or password in order to retrieve a file. |
| DIR | catalog | Retrieves a directory of the files and magic names available through the catalog.<br>Example:<br>`DIR public` |
| LIST | [listname] [list password] | Provide information about a mailing list. If the list's name is not provided, then a summary of all lists is returned. If the lists password is provided then a greater level of information about the list is returned.<br>Example:<br>`LIST MyList@example.com Lz$12` |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

**See:**

**Remote Server Control Via Email** 504
**Account Access and Control** 504
**General Email Controls** 509

### 11.2.3 General Email Controls

These are general email commands that can be sent to the system account via email messages. For more on using these sorts of commands, see: Remote Server Control via Email 504.

| COMMANDS | PARMS | DESCRIPTIONS |
|---|---|---|
| HELP | none | A copy of the NEWUSERHELP.DAT is processed and mailed back to the message originator. |
| RESULTS TO | address | The results of subsequent instructions are redirected to the email address specified rather than to that of the message originator.<br><br>Example:<br><br>`RESULTS TO user1@example.com`<br>`LIST MDSUPP` |
| STATUS | none | A status report on server operations and current conditions will be mailed back to the message originator. Since the information contained in this status report is considered private, the user requesting the report must be authenticated as an administrator.<br><br>Example: `STATUS` |

**See:**

**Remote Server Control Via Email** 504
**Account Access and Control** 504
**Mailing List and Catalog Control** 506

## 11.3 The RAW Message Specification

### 11.3.1 The RAW Message Specification

MDaemon has inherent support for a simple and powerful mail message format known as RAW mail. The purpose of the RAW mail system is to provide a simple and standard

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

format that software systems such as MDaemon can use to create much more complex RFC-2822 compliant message. Use of mail transport agents such as RAW allow client software to offload to the server all the complicated work of maintaining adherence to Internet mail standards.

RAW mail consists of a series of required and optional text headers followed by a message body. Most headers consist of a token followed by a value enclosed in <> symbols. Each header line ends with a <CRLF> combination of characters. Headers are separated from the message body by a blank line and are case insensitive, and the *from* and *to* headers are the only ones that are required. All text, headers and body, are plain ASCII text and must be contained in a file that ends with the extension, "`.raw`" (for example "`my-message.raw`"). Then, to queue the message for delivery, place the `*.raw` file in MDaemon's RAW queue (typically located at, "`C:\MDaemon\Queues\Raw`").

## Bypassing the Content Filter

By default, RAW messages are passed through the Content Filter like normal messages. If you want a given RAW message to bypass the filter then start the name of the file with "`p`" or "`P`". For example, "`P_my-message.raw`" would bypass the Content Filter but "`my-message.raw`" would be processed through it normally.

Bypassing the Content Filter will prevent messages from being DK or DKIM signed. If you have configured MDaemon to sign all messages then this could potentially cause some delivery problems. If you want MDaemon to sign RAW messages configured to bypass the Content Filter then you can do so by using the `x-flag=sign` option outlined below.

## RAW Headers

| | |
|---|---|
| From <mailbox@example.com> | This field contains the email address of the sender. |
| To <mailbox@example.com [, mailbox@example.com]> | This field contains the email address(es) of the recipient(s). Multiple recipients can be specified by separating each one with a comma character. |
| ReplyTo <mailbox@example.com> | An optional email address where replies to this message will be directed. |
| CC <maibox@example.com[, mailbox@example.com]> | An optional list of carbon copy recipients of this message. Multiple carbon recipients can be specified by separating each one with a comma character. |
| Subject <text> | An optional subject for the message. |
| Header <Header: Value> | Allows you to explicitly place Header/ |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Value combinations into the message. This makes it possible for you to place custom or other non-standard headers into your *.raw messages.

## Special Fields Supported by RAW

**File attachment and encoding**

`x-flag=attach <filepath, method> [-x]`

Example: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

This X-FLAG specifies the value "ATTACH" along with two parameters within the <> characters. The first parameter is a complete path to the file which should be attached to the message. The second parameter which is separated from the first by a comma character and specifies the method of encoding that is to be used when attaching the message. MDaemon supports two values for this parameter. The method of MIME instructs the server to use the Internet standard Base64 method of message encoding. The method of ASCII instructs the server to simply import the file into the message. An optional -X parameter at the end of the string instructs the server to remove the file from disk once it has been attached.

**Delivery Status Notification**

`x-flag=confirm_delivery`

When converting a RAW message which contains this flag into RFC-2822 mail, the string is transformed to the "Return-Receipt-To: <sender@example.com>" construct.

**Placing Specific Header/Value Combinations into the RFC-2822 Message**

`header <header: value>`

If you wish to place a specific header/value combination into the RFC-2822 message that will be generated from a RAW file, you will need to use the HEADER macro listed in the RAW Headers section above. For example, if you want the header "Delivered-By: mail-machine@example.com" to be placed into the RFC-2822 message you would place this: "header <Delivered-By: mail-machine@example.com>" in the RAW message. Note that the "header" macro requires both the field and value. You can place as many "header" macros as you need into a RAW message.

**DK/DKIM Signing RAW Messages**

`x-flag=sign`

Including this special command in a `*.raw` file will cause the RAW message to be DK/DKIM signed. This should only be used in RAW messages that you have configured to bypass the Content Filter (by starting their filenames with "`p`" or "`P`"). You should not use this command in normal RAW Messages that are

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

processed through the filter. Those messages will be signed normally.

All RAW messages that are generated by the Content Filter will use the `x-flag=sign` command automatically.

### Sample RAW mail messages

**Sample 1:**

```
from <mdaemon@altn.com>
to <user01@example.com>

Hello John!
```

**Sample 2:**

```
from <user01@example.com>
to <user09@example.net>
subject <Requested Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X

Here are all those files you asked for.
```

## 11.4 Semaphore Files

MDaemon is equipped with support for Semaphore Files, which can be used for a variety of purposes, including causing MDaemon to perform specific actions. Periodically MDaemon will scan the `\APP\` subfolder for the existence of these files. If it finds one, the associated behavior is triggered and the semaphore file is removed. This provides for a simple mechanism that enables administrators and developers to manipulate MDaemon without actually handling the interface. The following is a list of the semaphores and what they do:

| FILENAME | ACTION |
|---|---|
| ADDUSER.SEM | This semaphore creates new accounts. It is used to force MDaemon to append new records to the end of the `USERLIST.DAT` file without causing a potentially time consuming complete rebuild of the user database. Each line in this file must be a complete account record of the form specified in the Account Management Functions section of the MDaemon API (see `MD-API.html` in MDaemon's `\docs\API\` subfolder). Multiple new accounts can be specified – one account record per line. MDaemon will process |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| | the file one line at a time and add each new account. You can create ADDUSER.LCK to lock the file while you are updating it and MDaemon will not touch ADDUSER.SEM until ADDUSER.LCK is deleted. To see a sample ADDUSER.SEM file open ADDUSER.SMP in your APP directory with a text editor. |
| ALERT.SEM | Displays in a pop-up window the contents of the semaphore file to all WorldClient users who are logged in when the file is created. It is not, however, displayed to all users immediately—it is displayed to each user individually the next time his or her browser makes a request to the WorldClient server.<br><br>**Note:** Unlike other semaphore files, this file is WorldClient specific. Instead of placing it in the \app\ directory it must be placed in the \MDaemon\WorldClient\ directory. |
| ALIAS.SEM | Reloads aliases data file(s). |
| AUTORESPEXCEPT.SEM | Reloads the Autoresponder exception file(s). |
| BATV.SEM | Reloads Backscatter Protection (BATV) data file(s). |
| BAYESLEARN.SEM | This SEM manually starts the Bayesian learning process. This is like clicking the Learn button on the Bayesian tab of the Spam Filter. Note: this will start the Bayesian learning procedure even if you have Bayesian learning disabled. |
| BESBACKUP.SEM | This SEM initiates a backup of the BlackBerry Enterprise Server database, exactly like clicking the *Backup BlackBerry Enterprise Server database files* button at: BlackBerry Enterprise Server » Backup/Restore 177. |
| BESSLOWSYNC.SEM | Start a BlackBerry Enterprise Server (BES) slow sync operation. |
| BLACKLIST.SEM | Reloads the blacklist data files. |
| CATLIST.SEM | Reloads the internal cache of Catalog names. |
| CFILTER.SEM | Reloads Content Filter rules, clears Content Filter |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| | cached data, reloads the Spam Filter's White List (no filtering) 256 file. |
| CLEARQUOTACOUNTS.SEM | The results of user quota checks are maintained in the quotacounts.dat file. If you wish to clear the cached quota value for a user, add the user's email address to this SEM file and then place it in the \app\ folder. If an asterisk ( * ) is on a line by itself, the entire file will be deleted thereby invalidating all cached quota counts. |
| DELUSER.SEM | You can use this semaphore file to delete one or more user accounts. Create a text file containing the addresses of each account that you want to be deleted (one address per line), name the file DELUSER.SEM and then move it to MDaemon's \app\ directory. MDaemon will delete the accounts and then delete the DELUSER.SEM file. |
| DNS.SEM | Reloads the Windows DNS servers 51 and the Spam Filter's DNS settings. |
| DOMAINSHARING.SEM | Reloads domain sharing data file. |
| DYNAMICSCREENUPD.SEM | Adds entries to the DynamicScreen.dat file. Place the desired entries into this file and then MDaemon will manage adding them to the the DynamicScreen.dat file in the proper manner. |
| EDITUSER.SEM | This semaphore is used to update specific records within the USERLIST.DAT file without a potentially time consuming complete rebuild. To update a specific record within USERLIST.DAT you first construct a complete replacement record according to the format specified in the Account Management Functions section of the MDaemon API (see MD-API.html in MDaemon's \docs\API\ subfolder). The new record will reflect the changes that need to be updated within USERLIST.DAT. How does MDaemon know which record in USERLIST.DAT to update? This is accomplished by prepending the new record with the original record's email address followed by a comma. The EDITUSER.SEM file can contain multiple records to update – each on its own line. MDaemon will process the file one line at a time. You can create EDITUSER. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| | LCK to lock the file while you are updating it and MDaemon will not touch EDITUSER.SEM until EDITUSER.LCK is deleted. To see a sample EDITUSER.SEM file open EDITUSER.SMP in your \APP\ directory with a text editor. |
| EXITNOW.SEM | Shuts down MDaemon. |
| GATEWAYS.SEM | For optimal performance, MDaemon keeps its list of gateways in memory. Create a GATEWAYS.SEM in MDaemon's APP directory for it to reload the gateways.dat file. |
| GREYLIST.SEM | Reloads Greylisting data file(s). |
| GROUPS.SEM | Reloads account grouping data file(s). |
| GRPLIST.SEM | Reloads the internal cache of Mailing List names. |
| HANGUPG.SEM | Forces a conditional hang-up of RAS device. MDaemon will wait for any pending mail sessions to close and will then hang-up the RAS session. |
| HANGUPR.SEM | Forces unconditional hang-up of RAS device. This is an immediate and unconditional hang-up without regard to mail sessions which may be in progress across the connection. |
| HOSTSCREEN.SEM | Reloads Host Screen data file(s). |
| IPSCREEN.SEM | Reloads IP Screen data file(s). |
| IPSHIELD.SEM | The IPShield.dat file is cached in memory to increase access speed. Use IPSHIELD.SEM to reload the file into memory |
| LDAPCACHE.SEM | Reloads LDAP and gateway user data file(s). |
| LOCKSEMS.SEM | Prevents all semaphore file processing until user removes it. |
| LOGSETTINGS.SEM | Reloads log file settings. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| MDSPAMD.SEM | Reloads the Spam Filter white list and MDSPAMD, which forces it to reinitialize all its configuration data. |
| MINGER.SEM | Stops and then restarts the Minger[422] server. |
| MXCACHE.SEM | Reloads MX Cache data file(s). |
| NODNSBL.SEM | Reloads DNSBL white list file. |
| NOPRIORITY.SEM | Forces MDaemon to reload the `NoPriority.dat` file. |
| ONLINE.SEM | MDaemon will create this semaphore file once it makes a successful connection using RAS to the ISP. MD will remove the semaphore once the connection has been terminated. This is useful if you want to know when MD is using the RAS sub-system. |
| POSTDIAL.SEM | MDaemon will create this file immediately after a connection made by MDaemon is taken down. |
| PREDIAL.SEM | MDaemon will create this file just before trying to use RAS/DUN. This will allow other software to detect when it should free the dialup port so that MDaemon can use it. |
| PRIORITY.SEM | Reloads Priority mail data file(s). |
| PROCBAD.SEM | Initiates delivery of Bad Queue content. |
| PROCDIG.SEM | Initiates construction and delivery of mailing list digests. |
| PROCHOLDING.SEM | Initiates delivery of Holding Queue content. |
| PROCNOW.SEM | Initiates a check for remote mail and delivery of queued remote mail. |
| PROCREM.SEM | MDaemon will immediately go into mail processing mode and transact all remote mail. |
| PROCRETR.SEM | Initiates delivery of Retry Queue content. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| PRUNE.SEM | Reloads auto-pruning settings. |
| QUEUERUN.SEM | Just before a mail session begins MDaemon will create this semaphore file. Inside the file will be a datestamp indicating the time and date of the most recent mail processing interval. |
| RESTART.SEM | Stops and then starts MDaemon. |
| RESTARTCF.SEM | Stops and restarts CFEngine.exe (the Content Filter executable). |
| RELOADCACHE.SEM | Reloads all cached data settings and files except for Content Filter settings and files. |
| REVERSEEXCEPT.SEM | Reloads reverse lookups exception file. |
| SCHEDULE.SEM | Reloads schedule data file(s). |
| SPAMHONEYPOTS.SEM | Reloads spam honeypots data files(s) |
| SPF.SEM | Reloads SPF, DK, DKIM, and VBR data files(s). |
| SUPPRESS.SEM | Reloads black list settings and clears cached domain settings. |
| TARPIT.SEM | Reloads tarpit and dynamic screening data file(s). |
| TRANSLAT.SEM | Reloads the header translation data files. |
| TRAY.SEM | Redraws MDaemon's icon in the system tray. |
| TRUST.SEM | Trusted domains and IP addresses are kept memory resident for optimal performance. If you need to reload these settings manually you can create TRUST.SEM to do it. |
| UPDATEAV.SEM | Initiates SecurityPlus for MDaemon antivirus definition update. |
| UPDATESA.SEM | Initiates a Spam Filter update. |

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

| | |
|---|---|
| USERLIST.SEM | Reload the USERLIST.DAT file. Use this when you make modifications to the USERLIST.DAT and need MDaemon to reload it. |
| WATCHDOG.SEM | MDaemon will check for and remove this semaphore from the APP directory at approximately 10-20 second intervals. This file can be used by external apps to check if MDaemon is running. If this file remains in the APP directory for more than 20 seconds, that is a good indication that MDaemon is no longer running. |

## 11.5 Message Precedence System

This feature makes it possible for you to assign a "Precedence" value (level of importance) of 0 to 99 to messages. This value signifies the relative sort order of the messages during the delivery process. The lower the value, the higher its importance and the further up it will be in the sort order within a message queue. Thus, MDaemon will attempt to deliver a message with a value of 10 before one with a value of 90. As a guideline for assigning Precedence values: 10 = Urgent, 50 = Normal, and 80 = Bulk.

You will find options related to this feature on the Headers screen[200] under Preferences and on Options screen[431] of the Mailing List Editor. You can also use the Content Filter action, "*Add extra header item to message*[214]," to insert the Precedence header into any message.

## 11.6 Route Slips

A message file waiting in a queue typically contains within its headers all the information that is needed to get the message delivered to the proper location. There are headers stored within the file (such as the X-MDaemon-Deliver-To header) which provide MDaemon with instructions as to where and to whom the message should be delivered. Sometimes however it is necessary or useful to override this information and provide specific alternatives to where and to whom a message must be sent. Route Slips provide just such a mechanism. A route slip is a file that provides MDaemon with very specific instructions as to where and to whom a message should be sent. If a route slip is present for a particular message file then the settings within the route slip, and not those within the .MSG file itself, control where and to whom the message is sent.

Route slips end with the extension .RTE. For example, if a message file waiting to be sent is called "MD0000.MSG," then the corresponding route slip file for this message will be called MD0000.RTE and must be located in the same folder (mail queue) as the message file.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

The format of a route slip is as follows:

```
[RemoteHost]
DeliverTo=example.net
```

This section of a route slip provides MDaemon with the server to which the corresponding `.MSG` file is to be sent. MDaemon will always attempt a direct connection to this host attempting to route the message in as short a time as possible. Only one host may be specified.

```
[Port]
Port=xxx
```

This switch specifies the port that the TCP/IP connection and delivery attempt should be made on. Port 25 is the default for SMTP email.

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com

[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

These sections of the route slip allow you to specify any number of local and remote recipients who should receive a copy of the associated `.MSG` file. Local and remote recipient addresses must be kept separate and placed in their corresponding `[LocalRcpts]` and `[RemoteRcpts]` sections.

Route slips provide a good mechanism for delivering or redirecting email but they are not generally necessary. One use that MDaemon makes of route slips is in the case of "routed" mailing list mail. When you have a mailing list that is set to route a single copy of the list message to some remote host, a route slip is employed to accomplish this. It is a very efficient method of mail delivery when you have bulk addresses to deliver mail to since only a single copy of the message is required while any number of recipients of the message can be specified. Not all remote hosts allow this sort of routing to occur however. Since it is ultimately they who will have to deliver a copy of the message file to each address, some hosts place an upper limit on the number of recipients they will allow you to specify.

## 11.7 MDaemon and Proxy Servers

MDaemon was purposely designed to be highly versatile. Consequently, it can be configured for use with a wide variety of network configurations and various other products, and its flexibility allows it to work well with LAN proxy servers. To configure MDaemon to work through any proxy server, all you must do is make sure that the port settings (see Ports 491) you are using do not conflict with any that may be set in the proxy server itself. For example, SMTP email normally takes place on port 25. Since an IP address can only have a single port 25, two servers cannot both listen for SMTP

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

email at the same time on the same machine. When attempting to integrate MDaemon with a proxy, it is recommended that you allow MDaemon as much control over mail processing and delivery as possible. To that end, SMTP, POP, IMAP, and several other ports in the proxy may need to be disabled so that MDaemon can handle mail delivery independently.

However, should you find it necessary to channel mail through a proxy, MDaemon allows you to configure the ports which it will use to send and receive SMTP/POP/IMAP transactions. You may need to set these ports to non-standard values in order to filter your SMTP/POP/IMAP transactions through a proxy server or firewall.

For more detailed information on configuring MDaemon to work with a proxy server, please consult the support resources available at: www.altn.com.

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

# Section

# 12 Glossary

**ACL—**Stands for **A**ccess **C**ontrol **L**ists. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access to your folders to other users whom also have accounts on your mail server. Further, you can set permissions governing the extent to which each user has control over those folders. For example, you can designate whether or not a user is allowed to delete messages, flag them as read or unread, copy messages to folders, create new subfolders, and so on. Only email clients that support ACL can be used to share this access and set permissions. However, if your email client doesn't support ACL you can still set these permissions from the MDaemon interface.

ACL is fully discussed in RFC 2086, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2086.txt

**ASCII—**Pronounced as-key, ASCII is an acronym for "**A**merican **S**tandard **C**ode for **I** nformation **I**nterchange". It is the worldwide standard code for representing all upper and lower-case Latin letters, numbers, and punctuation as a 7 digit binary number, with each character assigned a number from 0 to 127 (i.e. 0000000 to 1111111). For example, the ASCII code for uppercase M is 77. The majority of computers use ASCII codes to represent text, which makes it possible for them to transfer data to other computers. Most text editors and word processors are capable of storing files in ASCII format (sometimes called ASCII files). However, most data files—particularly those containing numeric data—are not stored in ASCII format.

Several larger character sets have 128 additional characters because they use 8 bits instead of 7. These extra characters are used to represent symbols and non-English characters. The DOS operating system uses a superset of ASCII called extended ASCII or high ASCII. A standard that is closer to universal, however, is ISO Latin 1, which is used by many operating systems and Web browsers.

**ATRN—**See ETRN and ODMR below.

**Attachment—**A file attached to an email message. Most email systems only support sending text files as email, therefore if the attachment is a binary file or formatted text file (e.g. a word processor document), it must first be encoded as text before it is sent and then decoded once it is received. There are a number of encoding schemes—two of the most prevalent being Multipurpose Internet Mail Extensions (MIME) and Unix-to-Unix encode (Uuencode). For incoming messages, Alt-N's MDaemon server can be configured to either leave the decoding process to the recipient's email client or automatically decode attachments and store them in a specific location before delivering the message to the local user.

**Backbone—**A line or series of connections that form the major pathway within a network. This term is relative since the non-backbone lines in a large network might be larger than the backbone in a smaller network.

**Bandwidth—**The amount of data that can be transmitted in a fixed amount of time through a network or modem connection, usually measured in bits-per-second (bps). A full page of English text is about 16,000 bits, which a fast modem could transfer in

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

about 1 to 2 seconds. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

A good illustration of bandwidth is a highway. The highway represents the connection while the cars traveling on it represent the computer data. The wider the highway (the greater the bandwidth) the more cars that will be able to travel on it.

**Baud—**Baud rate is a measure of how frequently carrier signals change value on a phone line. It is a reference to the speed at which a modem transmits data. Usually, slower modems are described in terms of Baud rate while higher speed modems are described in bits per second. "Baud rate" and "bits per second" are not necessarily synonymous terms since each signal can encode more than one bit in high-speed connections.

**Bit—**A single **B**inary dig**it**. It is the smallest unit of computer data; a single digit number in base-2 (i.e. 0 or 1). It is usually abbreviated with a lower case "b" as in "bps" (bits per second). A full page of text is approximately 16,000 bits.

**Bitmap—**Most pictures you see on your computer, including all the ones found on the Internet, are bitmaps. A bitmap is a really just a map of dots (or bits) that looks like a picture as long as you're not to close to the screen, or have the bitmap magnified too much, to see the shape they make. Common Bitmap file types include BMP, JPEG, GIF, PICT, PCX, and TIFF. Because bitmap images are made up of a bunch of dots, if you zoom in on a bitmap it looks blocky rather than smooth. Vector graphics (usually created in CorelDraw, PostScript, or CAD formats) scale up much better because they are geometric shapes generated mathematically rather than simply being made of seemingly "random" dots.

**Bps—**"**B**its **P**er **S**econd" is a measurement of how fast computer data can be moved from one place to another. For example, a 33.6 kbps modem can transfer 33,600 bits per second. Kilobits (1000 bits) per second and megabits (1.000,000 bits) per second are abbreviated "Kbps" and "Mbps" respectively.

**Browser—**Short for "Web browser", it is an application used to display web pages. It interprets HTML code, text, hypertext links, images, JavaScript, and so on. The most widely distributed browsers are Internet Explorer and Netscape Communicator.

**Byte—**A set of bits (usually eight) that represent a single character. There are 8 bits in a byte, sometimes more, depending on how the measurement is being made. "Byte" is abbreviated with an uppercase "B".

**Cache—**Pronounced like "cash". There are various types of caches, but all are used to store recently used information so that it can be accessed quickly later. For example, a web browser uses a cache to store the pages, images, URLs, and other elements of web sites that you have recently visited. When you return to a "cached" page the browser will not have to download these elements again. Because accessing the cache on your hard disk is much faster than accessing the Internet, this significantly speeds up browsing.

MDaemon's IP Cache stores the IP addresses of domains to which you have recently delivered messages. This prevents MDaemon from having to lookup these addresses again when delivering additional messages to the same domains. This can greatly

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

speed up the delivery process.

**CGI—C**ommon **G**ateway **I**nterface is a set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. However, a CGI program is usually a small program that takes data from a web server and does something with it, like putting the content of a form into an email message, or doing something else with that data. CGI programs are often stored in a web site's "cgi-bin" directory and therefore appear in a URL that accesses them, but not always.

**cgi-bin—**The most common name of the directory on a web server in which CGI programs are stored. The "bin" part of "cgi-bin" is short for "binary" because most programs used to be referred to as "binaries". In reality, most cgi-bin programs are text files; scripts executed by programs located elsewhere.

**CIDR—**"**C**lassless **I**nter-**D**omain **R**outing" is a new IP addressing system that replaces the older system, which was based on classes A, B, and C. CIDR IP addresses look like normal IP addresses followed by a slash and number, called the IP prefix. For example:

123.123.0.0/12

The IP prefix defines how many addresses are covered by the CIDR address, with lower numbers covering more addresses. In the above example, the IP prefix of "/12" can be used to address 4,096 former Class C addresses.

CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

CIDR is addressed in RFCs 1517-1519, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

**Client—**A software program that is used to contact and obtain data from or send data to a *server* software program. The server is usually located on another computer, either on your local network or at some other location. Each *client* program is designed to work with one or more specific kinds of *server* programs, and each server requires a specific kind of client. A web *browser* is a specific kind of client that communicates with web *servers*.

**Common Gateway Interface—**See CGI above.

**Cookie—**In computer terminology, a *cookie* is data sent by a web server to your web browser, which is saved and later used for various purposes when you return to the same site or go to another location on the site. When a web server receives a request from a web browser that includes a cookie, it is able to use the information the cookie contains for whatever purpose it was designed, such as customizing what is sent back to the user, or for keeping a log of the user's requests. Typically,

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

cookies are used for storing passwords, usernames, preferences, shopping cart information, and similar things related to the site to which they correspond so that the site can appear to "remember" who you are and what you've done there.

Depending on your browser's settings, you may accept or not accept the cookies, and save them for various amounts of time. Usually cookies are set to expire after a predetermined amount of time and are saved in memory until the web browser software is closed down, at which time they may be saved to disk.

Cookies **cannot** read your hard drive. They can, however, be used to gather information about you related to your usage of their particular web sites, which would be impossible without them.

**Dial-up Networking—**A component in Windows that enables you to connect your computer to a network via a modem. Unless your computer is connected to a Local Area Network (LAN) with access to the Internet, you will need to configure Dial-Up Networking (DUN) to dial a Point of Presence (POP) and log on to your Internet Service Provider (ISP) before you will have Internet access. Your ISP may need to provide certain information, such as the gateway address and your computer's IP address.

DUN is accessed through the My Computer icon. A different dialup profile can be configured for each online service that you use. Once configured, you can copy a profile shortcut to your desktop so that all you need to do to make a connection is double-click the connection icon.

**Default—**This term is used to refer to the preset value for options in computer programs. Default settings are those settings which are used when no specific setting has been designated by the user. For example, the default font setting in Netscape Communicator is "Times". This setting will remain "Times" unless you change it to something else. Default settings are usually the value that most people will choose.

Frequently the term *default* is also used as a verb. If a custom setting won't work or the program lacks some needed bit of data for completing a task, it will usually "default" to a specific setting or action.

**DHCP—**An acronym for "**D**ynamic **H**ost **C**ontrol **P**rotocol". Network servers use this protocol to dynamically assign IP addresses to networked computers. A DHCP server waits for a computer to connect to it and then assigns it an IP address from a stored list.

DHCP is addressed in RFC-2131, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2131.txt

**Domain Gateway—**See Gateway below.

**Domain Name—**This is the unique name that identifies an Internet web site. For example, "altn.com" is the domain name of Alt-N Technologies. Each domain name contains two or more parts separated by dots; the leftmost part is the most specific while the rightmost part is the most general. Each domain name also points to the IP address of a single server, but a single server may have more than one domain

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

name. For example, "mail.altn.com", "alt-n.com", and "example.com" could all point to the same server as "altn.com", but "altn.com" could not point to two different servers. There are, however, methods for designating alternate servers to which clients will be directed if the main server goes down or is otherwise unavailable.

It is also common for a domain name to be registered but not be connected to an actual machine. The usual reason for this is the domain name's owner hasn't created a web site yet, or so that they can have email addresses at a certain domain without having to maintain a web site. In the latter case, there must be a real Internet machine to handle the mail of the listed domain name.

Finally, it is common to see the term "domain name" shortened and referred to as simply "domain". The word "domain" has other meanings and can refer to other things, such as a Windows NT domain or a class of values, so you should be aware of the distinction in order to avoid confusion.

Domain Names are addressed in RFCs 1034-1035, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

**DomainPOP—**Developed by Alt-N Technologies to be a part of the MDaemon server, DomainPOP makes it possible to provide email services for an entire LAN or workgroup from a single ISP POP mailbox. In the past, unless a company's email server had on constant "live" connection to the Internet, the only way to provide Internet email services to a workgroup was for each person to have their own mailbox on the company's ISP from which they could collect their mail. With DomainPOP only a single mailbox is required. The ISP pools all mail for the company's domain name into the mailbox from which it is periodically collected by DomainPOP. Then, DomainPOP parses the messages to determine the intended recipients of each and distributes them to the appropriate local user mailboxes. Thus email is provided for an entire network from a single dialup ISP account.

**Download—**The process by which your computer retrieves or obtains data from another computer. For example, information is obtained from the Internet by *downloading* it from other computers. The reverse of this is *uploading*. If you wish to send information to another computer then you will *upload* it to them.

**Driver**—A small program that communicates with a certain hardware device. Drivers contain information needed by the computer and other programs to control and recognize the device. Windows-based computers often have drivers packaged as a dynamic link library (DLL) file. Most hardware devices used with Macs do not need drivers, but when a driver is necessary it will usually come in the form of a System Extension.

**DUN—**See Dial-up Networking above.

**Email—**Stands for "Electronic mail". This term also appears in the forms: "E-mail", "e-mail", and "email"; all have the same meaning. Email is the transmission of text messages over communications networks. Most computer networks have some form of email system. Some email systems are confined to a single computer network, but others have gateways to other networks (which enables them to communicate with

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

multiple locations), or to the Internet (which enables them to send email anywhere in the world).

Most email systems include some form of *email client* (also referred to as a *mail client* or just *client*) which contains a text editor and other tools for composing messages, and one or more *servers* which receive the email from the clients and route it to its appropriate destination. Typically, a message is composed using the client, passed to a server for delivery to the *email address* (or addresses) specified in the message, and then routed by the server to another server that is responsible for storing messages destined for that address. If the message's destination is a local address for which the original server is responsible then it may be stored on the original server rather than routed to another. Last, the recipient of the message will connect to their server and retrieve the message by using their email client. This entire process of transferring an email message from your client to its destination server usually only takes a few seconds or minutes.

Besides containing simple text, email messages may also include file *attachments*. These attachments can be any type of file that you desire: pictures, text files, program files, other email messages, and so on. However, since most email systems only support sending text files, attachments must first be encoded (converted to a text format) before they can be sent, and then decoded when they arrive at their final destination. This process is usually done automatically by the sending and receiving mail clients.

All Internet Service Providers (ISPs) offer email. Most also support gateways so that you can exchange email with users of other email systems. Although there are many different protocols used for processing email by many different email systems, several common standards make it possible for users on virtually all systems to exchange messages.

**Email Address—**A name or string of characters that identifies a specific electronic mailbox on a network to which email can be sent. Email addresses are the locations to and from which email messages are sent. Email servers need email addresses so that they can route messages to their proper destinations. Different types of networks have different formats for email addresses, but on the Internet all email addresses have the form: "mailbox@example.com".

For example,

```
Michael.Mason@altn.com
```

**Email Client—**Also called a *mail client* (or just *client*), an *email client* is a software application that enables you to send, receive, and organize email. It is called a client because email systems are based on client-server architecture; a client is used to compose the email and then send it to a server, which then routes it to the recipient's server from which it will be retrieved by the recipient's client. Usually, email clients are separate software applications installed on the user's machine, but products such as Alt-N Technologies' WorldClient Server contain a built in client that is "served" to the user's web browser. Thus, their browser is used as the client rather than needing to install one on their machine. This greatly enhances the portability and convenience of email.

**Encryption—**A security measure, *encryption* is the coding or scrambling of information

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

in a file so that it will only be intelligible when it has been decoded or decrypted. Encryption is frequently used in email so that if a third party intercepted the email they would not be able to read it. The message is encrypted when it is sent and then decrypted at its final destination.

**Ethernet—**The most common type of connection used in a Local Area Network (LAN). Two of the most widely used forms of Ethernet are 10BaseT and 100BaseT. A 10BaseT Ethernet can transfer data at speeds up to 10 mbps (megabits per second) through a cable or wireless connection. A 100BaseT Ethernet transfers data at speeds up to 100 mbps. A Gigabit Ethernet can transfer data at rates up to 1000 mbps and is employed by some Apple computers.

**ETRN—**An acronym meaning **E**xtended **TURN**. It is an extension to SMTP that enables an SMTP server to send a request to another SMTP server to send, or "dequeue", mail that is being held for it. Because SMTP by itself cannot request mail (email is usually requested via the POP or IMAP protocols), this makes it possible for the SMTP server making the ETRN request to cause the remote server to start an SMTP session and begin sending the stored email to the host specified in the request.

The `TURN` command used for this purpose posed a security risk because it caused the SMTP session to reverse direction and begin sending the stored mail immediately without any verification or authentication that the requesting server was actually who it claimed to be. `ETRN` starts a new SMTP session rather than reversing direction. Thus if the server making the request is a "spoofed" host, the sending server will still attempt to deliver the mail to the real host instead. There is now a proposed standard that introduces Authenticated TURN (`ATRN`), which, like `TURN`, reverses the direction of the SMTP session but requires authentication before doing so. This new standard is On-Demand Mail Relay (ODMR). Alt-N Technologies' MDaemon server supports both ETRN and ODMR's ATRN.

ETRN is addressed in RFC 1985, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

**FAQ—**Pronounced together as "fack" or as separate letters "F-A-Q", FAQ stands for "**F**requently **A**sked **Q**uestions". FAQs are documents that provide answers to the most commonly asked questions on a given subject. They usually appear in some form of list format with each question listed first followed by its answer. In larger FAQs, oftentimes all of the questions will be listed at the beginning of the document with references (or hyperlinks, in online FAQs) to the location of the question and answer in the document. FAQs are frequently used as a starting point for technical support and instructions—a great deal of time and effort can be saved if you have access to a FAQ that answers your question instead of being forced to contact technical support.

**File Transfer Protocol—**See FTP below.

**Firewall—**In computer terminology, a *firewall* exists when you undertake security measures, through either software or hardware means, to separate a computer

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

network into two or more parts, or otherwise limit access to it to certain users. For example, you might want to let everyone view the home page of a web site hosted on your network but allow only your employees to get to an "employee only" area. Regardless of the method that you use to accomplish this—requiring a password, allowing connections from only certain IP addresses, or the like—the employee area is said to be behind a firewall.

**FTP—**Acronym for "**F**ile **T**ransfer **P**rotocol." It is a common and efficient method of transferring files via the Internet from one computer to another. There are specific client/server applications designed for this purpose called "FTP servers" and "FTP clients"—FileZilla, for example, is one of the most common clients. Usually FTP clients can perform quite a few other functions besides simply transferring files and are thus highly useful products. Some web browsers also contain support for File Transfer Protocol, though sometimes for downloading only. Additionally, most FTP servers are "anonymous FTP", which means that anyone can log in to them in order to download files—usually by specifying "anonymous" as the user name and then your email address as the password. Oftentimes you can download files from anonymous FTP sites without having to log in at all—they can be retrieved by simply clicking on a link. For browsers that support FTP, usually all that needs to be done is to connect to the FTP site using "ftp://..." in its URL rather than "http://..."

FTP is addressed in RFC-959, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc959.txt

**Gateway—**Computer hardware or software that translates data between two applications or networks with protocols that are dissimilar. "Gateway" is also used to describe any means by which access is provided from one system to another. For example, your ISP is a gateway to the Internet.

Alt-N Technologies' MDaemon Messaging Server can function as an email gateway for other domains through the use of its Domain Gateways feature. It acts as an intermediary, or Gateway, by collecting the domain's email and then holding it until the domain collects it. This is useful both for domains that do not maintain a continuous connection to the Internet and for domains that require a backup server in case theirs goes down.

**GIF—**"**G**raphics **I**nterchange **F**ormat" is a popular format for image files and is the most common format of images found on the Internet. GIF uses indexed colors or a palette of a certain number of colors, which greatly reduces file size—especially when the image contains large areas of the same color. The reduced size enables them to be quickly transferred between systems and accounts for their popularity on the Internet. The GIF compression formula was originally developed by CompuServe and thus you will often see GIF referred to as CompuServe GIF.

**Graphical User Interface—**See GUI below.

**GUI—**Pronounced "gooey", this acronym stands for "**G**raphical **U**ser **I**nterface". A GUI makes it possible to interact with your computer or application by using a pointing device to click graphical elements on the screen rather than typing in text at a command line. The Microsoft Windows and Apple Mac operating systems are both GUI-based, but—although first introduced by Apple—the idea of a graphical user interface actually originated from Xerox.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Host—**Any computer on a network that acts as a server for other computers on the same network. The host machine may be running a web server, email server, or other services, and it is common for it to provide several services at once. Host is also often used in the verb form "to host". For example, a machine running an email server would be "hosting" the email.

On peer-to-peer networks it is common for machines to be both hosts and clients at the same time. For example, your machine may host your network's printer but also be used by you as a client to collect email and download files from another host.

**HTML—**An acronym for "**H**ypertext **M**arkup **L**anguage. It is the coding language used to create Hypertext documents used on the World Wide Web. Simply put, an HTML document is a plain text document that contains formatting codes and tags that the user's web browser interprets and presents as a web page complete with formatted text and colors. For example, a browser receiving an HTML document containing the text "<B>Text</B>" would present the word "Text" in Bold. Because plain text files are very small, this makes it possible for them to be quickly transferred over the Internet.

**HTTP—H**yper**t**ext **T**ransfer **P**rotocol (HTTP) is the protocol used for transferring *hypertext* files between computers over the Internet. HTTP requires a client program on one end (usually a web browser) and an HTTP server on the other end.

HTTP is addressed in RFC-2616, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2616.txt

**Hypertext—**Any text that contains a hyperlink or jump to another document or place within the same document is called hypertext. Sometimes the text is also called a hypertext link or simply link. Hypertext can be either a word or phrase and has the link embedded in it so that clicking it will move you to the "book marked" location or cause the linked document to be displayed. Usually hypertext links are apparent because the text is underlined and a different color, but that is not required. Sometimes hypertext will look no different than normal text, but will almost always be indicated by some sort of graphical change to your pointer when the mouse pointer is paused over it.

**Hypertext Markup Language—**See HTML above.

**IMAP—**Developed by Stanford University, **I**nternet **M**essage **A**ccess **P**rotocol (IMAP) is a protocol used for managing and retrieving email messages. The latest version is IMAP4 and is similar to POP3 but with a number of additional features. IMAP4 is best known as a protocol used for managing email messages on the server rather than on the user's local machine—messages can be searched for keywords, organized in folders, specifically selected for downloading, and other features, all while they are still on the server. Thus IMAP places less demand on the user's machine and centralizes email so that it can be accessed from multiple locations.

IMAP is addressed in RFC-2060, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2060.txt

**IMAP4 ACL extension—**See ACL above.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Internet—**The Internet was created in 1969 by the United States military, originally to be a communications network that couldn't be destroyed during a nuclear war. It now consists of millions of computers and networks all over the world. By design, the Internet is decentralized—it is not controlled by any company, organization, or country. Each host (or machine) on the Internet is independent of the others and can provide whatever information or services its operators wishes to make available. Nevertheless, most information transferred over the Internet at some point passes through "backbones", which are extremely high-bandwidth high-speed connections controlled by the largest Internet Service Providers and organizations. Most people access the Internet through an online service such as AOL or through an Internet Service Provider (ISP) that maintains or is connected to one of these backbones.

Many people believe that the *World Wide Web* (WWW) and the Internet are the same thing, but this is not the case. The WWW is only one part of the Internet not the Internet itself. It is the most visible and popular part, largely driven by commerce, but still only a part.

**Intranet—**Simply put, an intranet is a small or private Internet used strictly within a company or organization's network. Although intranets vary widely from organization to organization, they may contain any of the features available on the Internet. They may have their own email systems, file directories, web pages to be browsed, articles to be read, and so on. The primary difference between an intranet and the Internet is that an intranet is relatively small and confined to an organization or group.

**IP—**An acronym for "**I**nternet **P**rotocol" (e.g. as in TCP/IP). Internet protocols make it possible for data to be transferred between systems over the Internet. Regardless of each machine's platform or operating system, if the same Internet Protocol is used by each machine then they will be able to transfer data to each other. The term "IP" is also commonly used as a further abbreviation of the term "IP Address". The current standard Internet Protocol is IP version 4 (IPv4).

Internet Protocol is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

**IP Address—**Occasionally called an IP Number, IP Address stands for **I**nternet **P** rotocol Address and is used to identify a particular TCP/IP network and the hosts or machines on that network. It is a 32-bit numeric address containing four numbers between 0 and 255 separated by dots (e.g. "127.0.0.1"). Within an isolated network, each computer must have a unique IP address, which can be assigned at random. But, every computer on the Internet must have a registered IP address to avoid duplication. Each Internet IP address can be either static or dynamic. Static addresses do not change and always represent the same location or machine on the Internet. Dynamic IP addresses change and are usually assigned by an ISP to computers that are only on the Internet temporarily—such as when a user with a dial-up account accesses the Internet. However, it is still possible for a dial-up account to have a static IP address assigned to it.

ISPs and large organizations usually attempt to acquire a range or set of IP addresses from the InterNIC Registration Service so that all clients on their network or using their service may have similar addresses. These sets are broken up into three classes: Class A, B, and C. Class A and B sets are used by very large

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

organizations and support 16 million and 65,000 hosts respectively. Class C sets are for smaller networks and support 255 hosts. Class A and B sets are now very difficult to get due to the shortage of available addresses; consequently most companies have to settle for multiple class C sets instead. Because of this IP address shortage, there is a new IP address protocol called Classless Inter-domain Routing (CIDR) that is gradually replacing the older system.

The current Internet Protocol standard, IPv4, is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

IP version 6 (IPv6) is addressed in RFC-2460 at:

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDR is addressed in RFCs 1517-1519 at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

**IP Number—**See *IP Address* above.

**ISP—**An **I**nternet **S**ervice **P**rovider (ISP) is a company that provides Internet access and services to the end user. Most ISPs provide multiple Internet services to their customers, such as: WWW access, email, access to newsgroups and news servers, and so on. Typically, users will connect to their ISP via dial-up, or some other form of connection, and then the ISP will connect them to a router, which will in turn route them to the Internet backbone.

**Java—**Developed by Sun Microsystems, Java is a network-oriented computer programming language with syntax much like C/C++ but is structured around classes instead of functions. In Internet applications it is commonly used for programming applets, which are small programs embedded in web pages. These programs can be automatically downloaded and executed by a user's browser in order to provide a large number of functions that wouldn't ordinarily be possible with just HTML or other scripting languages, and without fear of viruses or harm to your computer. Because Java is both efficient and easy to use, it is becoming popular among many software and hardware developers.

**JavaScript—**Not to be confused with Java, JavaScript was developed by Netscape as a scripting language designed to extend the capabilities of HTML and create interactive web pages. It is a highly pared down and easy to use programming language, which makes it much easier to use than Java and other languages but also limits it to some degree. It spite of its limitations it is very useful for adding a number if interactive elements to web sites. For example, JavaScript is useful when you want data to be preprocessed before it is submitted to the server, or when you want your pages to respond to user interaction with links or form elements. It can also be used to control plug-ins and applets based on user choices, and to accomplish a large number of other functions. JavaScript is included within the text of HTML documents and is interpreted by web browsers in order to perform the

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

functions.

**JPEG—**A graphics file format that is very efficient at compressing high-color and photographic images—much more so than the GIF format. While GIF is the best choice for images containing regular shapes and large areas of repeating color patterns, JPEG is much more suited to images with irregular patterns and large numbers of colors. JPEG is the most commonly used format for high-color and photographic images on the Internet. The acronym JPEG stands for "**J**oint **P**hotographic **E**xperts **G**roup"—the group that developed the format.

**Kbps—**Commonly used when referring to modem speeds (e.g. 56 Kbps), this acronym stands for "**K**ilo**b**its **P**er **S**econd". It is the number of kilobits (1000 bits) of data being moved or processed every second. Note that this is kilo*bits* not kilo*bytes*—a kilobyte would be eight times more data than a kilobit.

**Kilobyte—**A kilobyte (K or KB) is a thousand bytes of computer data. Technically it is 1024 bytes (2^10 = 1024) but in normal usage it is usually rounded off to 1000 for simplicity.

**LAN—**A **L**ocal **A**rea **N**etwork (LAN) is a computer network limited to a single building or area, usually having all nodes (computers or workstations) connected together with some configuration of wires or cables or some other form of media. Most large companies have a LAN, which greatly simplifies the management and sharing of information amongst employees and offices. Most LANs utilize some form of email or chat system, and share devices such as printers in order to avoid having to have a separate device for each station. When the network's nodes are connected together via phone lines, radio waves, or satellite links it is called a Wide Area Network (WAN) instead of LAN.

**Latency—**The time it takes a data packet to move across a network connection. While a data packet is being sent, there is "latent" time during which the sending computer waits for a confirmation that the packet has been received. In addition to bandwidth, latency is one of the factors that determine the speed of your connection.

**LDAP—L**ightweight **D**irectory **A**ccess **P**rotocol (LDAP) is an online directory service protocol that is a simplification of Directory Access Protocol (DAP). The directory system is in a hierarchical structure consisting of the following levels: The "root" or starting directory, country, organization, organizational unit, and individual within that unit. Each LDAP entry is a collection of attributes with a unique identifier, called a distinguished name (DN). Because it is an open protocol, is efficient, and has the ability to be distributed across many servers, LDAP may eventually make it possible for virtually any application on any platform to access directory information for locating email addresses, organizations, files, and so on worldwide.

LDAP is addressed in RFC-2251, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2251.txt

**Link—**See *Hyperlink* above.

**List server—**A server application that is used to distribute email messages to multiple recipients by simply addressing the message to a single address. Simply put, when

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

an email message is addressed to a *mailing list* maintained by the list server it will be automatically broadcast to the members of the list. Mailing lists typically have a single normal email address (for example, listname@example.com) but that address refers to a whole list of recipients rather than to a specific person or mailbox. When someone *subscribes* to a mailing list, the list server will automatically add the address to the list and distribute future emails directed to the list to that address, or member, and all other members. When someone unsubscribes, the list server simply removes the address so that it will receive no further list messages.

Frequently the term listserv is used generically to refer to any mailing list server. However, Listserv® is a registered trademark of L-Soft international, Inc. and is a specific program developed by Eric Thomas for BITNET in 1986. Besides other list servers, Alt-N Technologies' MDaemon server is equipped with an entire suite of list server, or mailing list, functions and features.

**Logon—**a unique code or series of characters used to gain access or otherwise identify yourself to a server or machine. In most cases a password must accompany the logon in order to gain access.

There are many terms used synonymously with "logon", such as *login*, *username*, *user name*, *user ID*, *sign-in*, and others. Frequently, "logon" is also used as a verb. For example, "I am going to *logon* to the mail server". In that context, however, the more common usage (and perhaps more proper) is "I am going to *log on* to the mail server".

**Mailbox—**An area in memory or on a storage device that is assigned to a specific email address and where email messages are stored. In any email system, each user has a private mailbox in which messages are stored when that user's mail server receives them. It is also common for the term "mailbox" to be used when referring to the leftmost portion of an email address. For example, "user01" in "user01@example.com" is the mailbox while "example.com" is the domain name.

**Mailing List—**Also called email groups, a mailing list is a list or group of email addresses identified by a single email address. For example, "listname@example.com". Typically when a list server receives an email message addressed to one of its mailing lists that message will be automatically distributed to all of the list's members (i.e. the addresses included in the list). Alt-N Technologies' MDaemon server is equipped with an extensive suite of mailing list features that enable lists to be public or private (anyone can post or join, or only members can post or join), moderated (each message must be approved by someone before it will go to the list), sent in digest format or as individual messages, and used in a variety of other ways.

**Megabyte—**Though technically 1,048,576 bytes (or 1024 kilobytes), a megabyte is more commonly rounded off and used to refer to a million bytes. Megabyte is abbreviated: "MB", as in "20 MB".

**MIME—**Defined in 1992 by the Internet Engineering Task Force (IETF), **M**ultipurpose **I**nternet **M**ail **E**xtensions (MIME) is the standard encoding method used for attaching non-text files to standard Internet email messages. Because typically only plain text files can be transferred via email, non-text files must first be encoding into a plain text format and then decoded after reaching their destination. Thus, an email program is said to be MIME Compliant if it can both send and receive files using the MIME standard. When a MIME-encoded message attachment is sent, generally both

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

the type of file being sent and the method that should be used to turn it back into its original form are specified as part of the message. There are many predefined MIME content types, such as "image/jpeg" and "text/plain". However, it is also possible to define your own MIME types.

The MIME standard is also used by web servers to identify the files they are sending to web browsers. Because web browsers support various MIME types, this enables the browser to display or output files that are not in HTML format. Further, by updating the browser's lists of MIME-Types and the software used for handling each type, new file formats can be readily supported.

MIME is addressed in RFCs 2045-2049, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

**Mirror—**A server (usually an FTP server) that has a copy of the same files that are on another server. Its purpose is generally to provide an alternate location from which the mirrored files can be downloaded should the original server go down or be overloaded. The term "mirror" can also refer to a configuration whereby information is written to more than one hard disk simultaneously. This is used as a redundancy measure so that if one disk fails the computer can continue to operate without losing any vital data.

**Modem—**An acronym derived from **mo**dulator-**dem**odulator. A modem is a device connected to a computer that enables the transfer of data to other computers over telephone lines. The modem converts the computer's digital data to an analog format (modulates) and then transmits it to another modem where the process is reversed (demodulates). Put simply, a modem is an analog-to-digital and digital-to-analog converter. The speed at which the data is transferred is expressed in either baud-rate (e.g. 9600 baud) or kilobits per second (e.g. 28.8 kbps).

**MultiPOP—**A component of Alt-N Technologies' MDaemon Messaging Server that can be configured to collect email, via the POP3 protocol, simultaneously from various email servers on behalf of MDaemon's users. This makes it possible for MDaemon account holders who have email accounts elsewhere on other email servers to have that email collected and pooled with their MDaemon account email. Thus storing all of their email in a single mailbox.

**NAT—**See Network Address Translation below.

**Network—**Two or more computers connected together in some fashion. The purpose of a network is to enable the sharing of resources and information between multiple systems. Some common examples are: multiple computers sharing printers, DVD-ROM drives, hard disks, individual files, and so on.

There are many types of networks, but the most broadly defined types are Local

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Area Networks (LANs) and Wide Area Networks (WANs). In a LAN, the individual computers (or nodes) are geographically close together—usually in the same building. They are also usually connected together directly with wires, although wireless connections are becoming common as well. The nodes in a WAN are usually farther apart (in another building or city) and connected via telephone lines, satellite hook-up, or some other form of connection.

The Internet itself is a network. It is often described as a network of networks.

**Network Address Translation—**Network address translation (NAT) is a system whereby two sets of Internet Protocol addresses (IP addresses) are used by a single network —one for external traffic and the other for internal traffic. This is mainly used as a firewall measure to help ensure network security. Your computer will appear to have a certain IP address to computers outside your LAN while your actual IP address is altogether different. Hardware or software placed "between" your network and the Internet performs the translations between the two addresses. Using this method, it is common for multiple computers in a LAN to "share" one company IP address. Thus there is no way for someone outside your network to know your actual address and directly connect to your computer without it first being qualified or authenticated during the translation.

**Network Interface Card—**A network interface card (NIC) is a computer circuit board that enables a computer to be connected to a network. NICs provide a full-time network connection whereas a modem (used by most home computers to dial-in to a network via telephone lines) usually provides only a temporary connection. Most NICs are designed for specific types of networks and protocols, such as Ethernet or token ring and TCP/IP.

**Network News Transfer Protocol—**See NNTP below.

**NIC—**See Network Interface Card above.

**NNTP—N**etwork **N**ews **T**ransfer **P**rotocol (NNTP) is the protocol used to transfer and distribute messages on USENET newsgroups. The most common and popular browsers and email clients now have NNTP clients built-in.

NNTP is addressed in RFC-977, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc977.txt

**Node—**Any single computer connected to a network.

**ODMR—O**n-**D**emand **M**ail **R**elay is a new protocol designed to enable mail servers with only an intermittent connection to a service provider, and which do not have a static IP address, to receive mail similarly to those servers that do have one and use the ETRN command. If the system has a static IP address, the ESMTP ETRN command can be used. However, systems with dynamic IP addresses have no widely deployed solution. ODMR solves this problem. Among other things, ODMR introduces the Authenticated TURN command (ATRN) which causes the flow of an SMTP session to be reversed (like the older TURN command) but with the added security of requiring that the requesting server be authenticated. This makes it possible for an SMTP server with a dynamic IP address to connect to its ISP and have one or more host's email delivered to it via SMTP rather than collect it via POP or IMAP. This

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

helps meet the widespread demand for a low-cost solution for those companies that need to their own mail server but cannot afford a static IP address or dedicated online presence.

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

**OEM—O**riginal **E**quipment **M**anufacturer (OEM) is an often confusing and misunderstood term. An OEM is a company that uses another company's equipment or products in its own product that is packaged and sold under a different brand or company name. For example, HyperMegaGlobalCom, Inc. is an OEM because it purchases computer components from one or more different companies, puts them all together into a single customized product, and then sells it with "HyperMegaGlobalCom" stamped on it. The company that sold HyperMegaGlobalCom the components might also be an OEM if they in turn got their components from someone else as well. "OEM" is an unfortunate misnomer because OEMs are not actually the original manufacturers; they are the "packagers" or "customizers". In spite of this, many people still often use the term "OEM" when referring to the actual hardware manufacturers instead of those who repackage it—and understandably so.

**On the fly—**The term "on the fly" is commonly used it two different ways. First, it is often used to denote something that can be done "in a hurry" or easily while "in the middle" of performing some other task. For example, a bookkeeping product might support creating accounts "on the fly" while in the middle of entering sales figures —"Simply stop entering figures, click button X, enter a name, and then continue entering more figures." The other way that "on the fly" is used is in referring to something that can be generated dynamically or automatically instead of manually or statically. For example, by using the information stored in a "cookie" a customized web page might be generated "on the fly" when a user returns to a web site. Rather than requiring someone to manually create a page customized to the user's tastes, it would be generated dynamically based upon that person's actions while browsing.

**Original Equipment Manufacturer—**See OEM above.

**Packet—**A unit of computer data sent over a network. Any time you receive data from another computer on your LAN or over the Internet it comes to your computer in the form of "packets". The original file or message is divided into these packets, transmitted, and then recombined at the destination. Each packet contains a header containing its source and destination, a block of data content, and an error-checking code. It is also "numbered" so that it can be connected to related packets being sent. The process of sending and receiving packets is known as "packet-switching". Packets are also commonly called "datagrams".

**Packet Switching—**The process of sending and receiving packets over a network or the Internet. In contrast to circuit switching (such as in an analog telephone), which sends the data in a continuous stream over a single path or circuit, packet switching transmits the data broken up into "packets", which may not necessarily take the same route to get to their destination. Further, because the data is in separate units, multiple users can send different files simultaneously over the same path.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

**Parameter—**A parameter is a characteristic or value. In computing, it is any value passed to a program by a user or another program. Your name and password, a preference setting, font size, and so on are all parameters. In programming, a parameter is a value that is passed to a subroutine or function for processing.

**PDF—P**ortable **D**ocument **F**ormat (PDF) is a highly compressed multi-platform file format developed by Adobe Systems Incorporated that captures document formatting, text, and images from a variety of applications. This makes it possible for the document to appear the same and print accurately on multiple computers and platforms (unlike many word processors). Viewing a PDF file requires the Adobe Acrobat Reader, a free application distributed by Adobe Systems. There is also a plug-in for viewing PDF files with your web browser. This makes it possible to view PDF files posted on a web site directly instead of having to download them first and then view them with a separate program.

**Parse—**In linguistics, to parse is to divide language into its grammatical components that can be analyzed. For example, dividing a sentence into verbs, adjectives, nouns, and so on.

In computers, to parse is to divide a computer language statement into parts that can be made useful for the computer. A parser in a compiler is takes each program statement that a developer has written and divides it into parts that can then be used for developing further actions or for creating the instructions that form an executable program.

Alt-N Technologies' MDaemon server and other products often parse email messages to determine their destination or to process them through filters and other tools.

**Ping—**An acronym for **P**acket **In**ternet **G**roper. It is a basic Internet program used to determine whether a specific IP address is reachable and accepting requests. It does this by sending an Internet Control Message Protocol (ICMP) Echo request and waiting for a response. "Ping" is commonly used as a verb when referring to this process. For example, "I am going to ping that server to see if it is online." "Pinging" an IP address is usually as simple as typing "ping" followed by the IP address or domain at the DOS prompt. For example "Ping 192.0.2.0."

ICMP is addressed in RFC-792 and the Echo protocol is addressed in RFC-862. These can be viewed at:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

**POP—**Stands for **P**ost **O**ffice **P**rotocol. POP (also commonly appears as POP3) is the most commonly used email protocol for retrieving email from a mail server. Most email clients use the POP protocol although some also support the newer IMAP protocol as well. POP2 became a standard in the mid 1980s and required SMTP to send messages. It was replaced by the newer version, POP3, which can be used with or without SMTP. POP is sometimes used as a verb when referring to collecting your email from a server. For example, "I'm going to POP my mailbox to get my mail."

POP3 is addressed in RFC-1939, which can be viewed at:

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

http://www.rfc-editor.org/rfc/rfc1939.txt

**Port—**In TCP/IP and UDP networks and the Internet, a port is the endpoint of a logical connection and is identified by a number from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged protocols and services. For example, web servers typically are listed on port 80, SMTP servers typically communicate on port 25, and POP servers send and receive mail on 25. Generally, only one program at a time can use, or "bind", to any given port on each machine. When browsing the Internet, oftentimes certain servers will be running on non-default ports, which require you to specify the port in the URL after a colon. For example, "www.example.com:3000."

Port can also be used to refer to the sockets on a computer used for connecting peripheral devices and hardware to it. For example, serial ports, parallel ports, USB ports, and so on.

Finally, port is often used to describe the process of making a program designed for a specific platform or machine function on another platform. For example, "to port a Windows application to UNIX" or "to create a UNIX port for an application."

**Post—**In Internet messaging, such as email or newsgroups, it is a single message entered into a network communications system for others to see. For example, a message displayed on a newsgroup, mailing list, or discussion board is a post. It can also be used as a verb, as in "post a message to the mailing list or on the newsgroup."

**PPP—**Stands for "Point to Point Protocol." It is the Internet standard for dial-up connections. PPP is a set of rules that defines how your modem connection exchanges packets of data with other systems on the Internet.

PPP is addressed in RFC-1661, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1661.txt

**Protocol—**In computing, a protocol is a set of guidelines or standards by which servers and applications communicate. There are many different protocols used for many different purposes, for example, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, and so on.

**Registry—**A database used by Microsoft Windows to store configuration information about software installed on the computer. This includes things like user settings, file extension associations, desktop background, color schemes, and many others. It has the following six parts:

HKEY_User—Stores user information for each user of the system.

HKEY_Current_User—Preferences for the current user.

HKEY_Current_Configuration—Stores settings for the display and printers.

HKEY_Classes_Root—File associations and OLE information.

HKEY_Local_Machine—Hardware, operating system, and installed application settings.

HKEY_Dyn_Data—Performance data.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

When programs are installed on your computer the installer usually writes some information to the registry automatically. You can manually edit the registry, however, by using the regedit.exe program that is built in to Windows. But, you should exercise extreme caution when doing this because altering the wrong setting in the registry could cause your computer to function improperly, or not at all.

**RFC—R**equest **F**or **C**omments is the name of the result and the process for creating a standard on the Internet. Each new standard and protocol is proposed and published on the Internet as a "Request For Comments." The Internet Engineering Task Force (IETF) facilitates discussions on the new standard and eventually it is established. In spite of the fact that the standard is established and no further "comments" are "requested," the standard still retains the "Request for Comment" acronym along with its identifying number. For example RFC-822 (now superseded by RFC-2822) is the official standard, or "RFC," for email. However, those protocols that are officially adopted as "standards" do have an official standard number associated with them that is listed in the Internet Official Protocol Standards document (which itself is STD-1 and currently RFC-3700). You can find RFCs on the Internet at many locations but the authoritative source is The RFC Editor, located at http://www.rfc-editor.org/.

The Internet Official Protocol Standards document is located at:

http://www.rfc-editor.org/rfc/std/std1.txt

**RTF—R**ich **T**ext **F**ormat is a universal file format developed by Microsoft that is supported by nearly all word processors. In contrast to plain text format, RTF enables you to retain formatting, font information, text color, and so on. The file size of RTF files can be very large when compared to other file formats such as Microsoft Word's format (*.doc and *.docx) and Adobe PDF.

**Server—**A computer, or program, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as an SMTP server, or a machine on which the software is running. A single server *machine* could have many different server *programs* running on it concurrently. For example, your network's server might be running a web server, email server, FTP server, fax server, and others all at once.

**SMTP—**An acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is the primary protocol used to send email on the Internet from one server to another or from a client to a server. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Once a server has received email via SMTP it is usually stored there and can then be retrieved by a client via the POP, IMAP, or other protocol.

The SMTP protocol is addressed in RFC-2821, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2821.txt

**Spam—**Junk mail on the Internet. "Spam" is most commonly used to refer to unsolicited bulk email, although it is often used to refer to any unwanted email in general. A "spammer" will obtain hundreds, thousands, or even millions of email addresses from various sources and then "spam" the list with a message or solicitation. "Spam" can, however, be used to refer to a newsgroup or discussion

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

board posting as well, when the posting is some unwanted or unrelated advertisement for a product or web site.

Spam is quickly becoming a serious problem on the Internet, tying up a great deal of time and server resources. And because spammers oftentimes use various techniques to attempt to mask the origin of the message—such as "spoofing" their addresses to appear to be someone else or attempting to relay the spam covertly through multiple mail servers—preventing it can be a challenge. Alt-N Technologies' MDaemon server is equipped with a number of features designed specifically to aid in fighting spam, such as: DNS Black Lists (DNS-BL), IP Shielding, IP Screening, Relay Control, and others.

The origin of using the term "Spam" to refer to junk email is debated, but it is generally accepted that it comes from a popular Monty Python sketch in which the word "spam" is repeated over and over and periodically accompanied by Vikings singing, "Spam spam spam spam, spam spam spam spam…" However, it may simply be a disparaging comparison to the trademarked Hormel meat product of the same name—everybody gets it at one time or another, but does anyone ever really ask for it?

**TCP/IP—T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) has been described as the foundation of the Internet. It is the basic suite of communication protocols used on the Internet to connect hosts. It is the most commonly used protocol on Local Area Networks as well. It is a two-layer system, the topmost layer being TCP, which manages the disassembling and assembling of files into packets for transmitting over the network. IP, which is the lower layer, handles the addressing of the packets so that they get to the proper destinations. TCP is addressed in the following RFC-793. IP is addressed in RFC-791. These RFCs can be found at:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

**Telnet—**A command and program used to log on to Internet sites that support Telnet access. The Telnet command gets you to the logon prompt of the Telnet server. If you have an account on that server, you can access your permitted resources such as your files, email, and so on. The downside of Telnet is that it is a command line program that uses Unix commands.

The TELNET protocol is addressed in RFCs 854-855, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

**Terminal—**A device that allows you to send commands to a remote computer. A terminal is a keyboard, display screen, and some simple circuitry. Oftentimes, however, personal computers are used to "emulate" terminals.

**Tiff—**An acronym for **T**agged **I**mage **F**ile **F**ormat. It is a graphics file format created to be a universal graphics translator across multiple computer platforms. TIFF can handle color depths ranging from 1-bit to 24-bit.

**UDP—U**ser **D**atagram **P**rotocol (UDP) is one of the protocols that make up the TCP/

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

IP suite of protocols used for data transfers. UDP is a known as a stateless protocol because it doesn't acknowledge that packets being sent have been received.

UDP is addressed in RFC-768, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc768.txt

**Unix—**Unix, or UNIX, is an operating system created by Bell Labs in the 1960s. Designed to be used by many users at the same time, it is the most popular operating system for servers on the Internet. There are now many different operating systems based on UNIX such as Linux, GNU, Ultrix, XENIX, and others.

**URL—**Every file or server on the Internet has a **U**niform **R**esource **L**ocator (URL). It is the address that you enter into your web browser to get to that server or file. URLs cannot have spaces and always use forward slashes. They have two parts separated by "://". The first part is the protocol being used or resource being addressed (for example, http, telnet, ftp, and so on) and the second part is the Internet address of the file or server (for example, www.altn.com or 127.0.0.1).

**Uuencode—**A set of algorithms for converting files into a series of 7-bit ASCII characters for transmission over the Internet. Although it stands for Unix-to-Unix encode, it is no longer exclusive to UNIX. It has become a universal protocol used to transfer files between different platforms. It is an encoding method commonly used in email.

**WAN—**A WAN, or **W**ide **A**rea **N**etwork, is similar to a Local Area Network (LAN) but is usually spread across multiple buildings, or even cities. WANs are sometimes composed of smaller LANs that are interconnected. The Internet could be described as the biggest WAN in the world.

**Zip—**Refers to a compressed or "zipped" file, usually with the "`.zip`" file extension. "Zipping" is compressing one or more files into a single archive file in order to save space for storage or to facilitate faster transfer to another computer. To use a zip file, however, you'll need to unzip it first with the appropriate program such as PKZIP or WinZip. There are multiple compression/decompression utilities available—both shareware and freeware—from many sites on the Internet. Hopefully you won't have to unzip the utility before you can install it.

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

# Index

## - A -


Access Control List 77, 79
Access Control Lists 373
Access Rights 79, 373
Account 343
  Database Options 411
  Notes 376
  Quotas 419
Account Access and Control 504
Account Aliases 398
Account Autoresponders 359
Account Database Options 411, 412
Account Defaults 380
Account Editor
  Access Control List 373
  Access Rights 373
  Account 359
  Administrator Notes 376
  Aliases 368
  Attachments 349
  Filters 356
  Folder 349
  Folder Access Rights 373
  Forwarding 362
  Groups 349
  Mail Services 345
  Mailbox 349
  Notes 376
  Options 377
  Quotas 366
  Shared Folders 373
  Web Services 346
Account Groups 420
Account Integration 425
Account Manager 340
Account permissions 346
Account Pruning 366
Account Signature 375
Account Templates 380, 383
Accounts 423, 425
  Account-specific BES options 351
  Autoresponders 390
  BES 176
  BIS 187, 353
  BlackBerry Internet Service 187, 353
  Defaults 380, 383, 385, 387
  DomainPOP 83
  Erasing a BlackBerry device 351
  Groups 420
  New 380, 385, 387
  ODBC Selector Wizard - Account Database 412
  Quotas 385
  Resynchronizing a BlackBerry device 351
  Sending a policy 351
  Slow Sync 176
  Template Macros 383
  Web Access Defaults 387
ACL 79
ACLs 373
Activating Outlook Connector 409
Activation 162
Activation options 179
Activation password 351
Active Directory 402, 406
  Creating Accounts 402
  Deleting Accounts 402
  Dynamic Authentication 402
  File Security 402
  Monitoring 404
  Options 406
  Persistent Monitoring 402
  Port (Gateway) 461
  Server (Gateway) 461
  Synchronization 404
  Synchronizing with MDaemon 402
  Template 402
  Updating Accounts 402
  Using with Mailing Lists 448
  Verification (Gateway) 461
ActiveSync
  Accounts 160, 355
  Account-specific Options 355
  Assigning Policies 159
  Default Policies 159
  Deleting Devices 160
  Domains 159
  Integrated Accounts 160
  Options 161
  Policies 156
  Remotely Wiping a Device 160


*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

ActiveSync
  Server 154
  Wiping Devices 160
ActiveSync Policy Editor 156
AD 448
AD Options 406
Adding Outlook Connector users 410
Address
  Blacklist 299
  Suppression 299
Address Aliases 368, 398
Address Aliases Options 400
Address Book Options 96
Address Book Synchronization 111
Address Books 418
Address Verification 422
Address Verification (Gateway) 461
Administrator
  Domain 377
  Global 377
  Notes 376
Admins/Attachments 223
Alias Editor 398
Aliases 368, 398
Aliases Options 400
ALL_USERS list macro 433
ALL_USERS:<domain> list macro 433
AntiSpam 236
AntiVirus 151, 231, 233, 235, 236
  Configuring updater 233, 235
  EICAR test message 233, 235
  Malware 233, 235
  Scheduler 151, 233, 235
  Testing 151, 233, 235
  Updater 151, 233, 235
  Urgent Updates 151, 233, 235
  Viewing update report 233, 235
Anti-virus 210
AntiVirus support 210
AntiVirus Updates 151, 152
APOP 46
Approved List 298
Archival 59
Archiving Logs 103
Archiving mail in a pre 92
ATRN 49, 57, 466
Attachment extension 195
Attachment Linking 142, 349
  BIS 189
  BlackBerry Internet Service 189
Attachment restricting 223
AUTH 57, 280
Authentication 280
Authentication-Results header 285
Authorizing Outlook Connector users 410
Auto Response Script Samples 396
Auto Response Scripts 393
Auto-generated a Spam Folder and Filter 267
Automatic
  Gateways 473
  IP Screening 328
  Log Archiving 103
Automatic Learning 249
automatically extracting attachments 142
automatically linking attachments 142
Autoresponder Exception List 391
Autoresponder Options 392
Autoresponders 359, 390, 393, 396
  Account list 390
  Overview 390
AV
  Alt-N AntiVirus for MDaemon 231
  AntiVirus tab 231
  AntiVirus Updater 233, 235
  SecurityPlus for MDaemon 233, 235
Available Disk Space 197

# - B -

Backing up logs 103
Backing up the BES database 177
Backscatter Protection 323
Backscatter Protection - Overview 322
Backup Server 461
Bad Messages 482
Balance 162, 167
Bandwidth 325
Bandwidth Throttling 325, 326
Base Entry DN 406, 448
BATV 322, 323
Bayesian
  Auto-learning 249
  Classification 245
  Learning 249
Bayesian Classification 241
Bayesian Learning 241, 245

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

BES 162
Account PIN 176
Account Status 176
Accounts 176
Account-specific options 351
Activation 162, 176
Activation options 179
Activation password 351
Applying a policy to a domain 174
Applying a policy to an account 351
Backup 177
Calendar options 179
Database Backup & Retore 177
Dialog 162
Disabling 166
Domain Policy 174
Domains 174
Enabling 166
Enterprise Activation 162
Erasing a device 351
Features 162
Integrated Accounts 176
IT Policies 167
Logging 179
MDS Connection Service 175
Options 179
Overview 162
Password 351
PIN 176
Policies 167
Policy 351
Policy Rules 167
Resending service books 351
Resetting a device's password 351
Resetting the calendar 179
Restore 177
Resynchronizing a device 351
Rules 167
Sending a policy 351
Service books 351
Services 166, 179
Setting a Domain's Policy 174
Slow sync 176, 179, 351
SRP 166
Status 166
Stopping when MDaemon stops 179
Synchronization options 179
Verifying SRP 166
Wiping a device 351
BIS 183
Accounts 187, 353
Attachment Linking 189
BlackBerry Internet Service 185
Domains 185
Filtering mail 353
Folders 189
History 185
Inbox 189, 353
Integration 187
Logs 189
Overview 183
Push mail 187, 353
SMTP Server 185
SSL 185
STARTTLS 185
SUBSCRIBE 187
Subscribe URL 185
UNSUBSCRIBE 187
Black List 241, 259
Black Lists 264
BlackBerry Balance 162, 167
BlackBerry Device Activation 162
BlackBerry Enterprise Server 162
Account PIN 176
Account Status 176
Accounts 176
Account-specific options 351
Activation 162, 176
Activation options 179
Activation password 351
Applying a policy to a domain 174
Applying a policy to an account 351
Backup 177
Calendar options 179
Database Backup & Retore 177
Dialog 162
Disabling 166
Domain Policy 174
Domains 174
Enabling 166
Enterprise Activation 162
Erasing a device 351
Features 162
Integrated Accounts 176
IT Policies 167
Logging 179

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

BlackBerry Enterprise Server 162
MDS Connection Service 175
Options 179
Overview 162
Password 351
PIN 176
Policies 167
Policy 351
Policy Rules 167
Resending service books 351
Resetting a device's password 351
Resetting the calendar 179
Restore 177
Resynchronizing a device 351
Rules 167
Sending a policy 351
Service books 351
Services 166, 179
Setting a Domain's Policy 174
Slow sync 176, 179, 351
SRP 166
Status 166
Stopping when MDaemon stops 179
Synchronization options 179
Verifying SRP 166
Wiping a device 351
BlackBerry Internet Service 183
Accounts 187, 353
Attachment Linking 189
BIS 185
Domains 185
Filtering mail 353
Folders 189
History 185
Inbox 189, 353
Integration 187
Logs 189
Overview 183
Push mail 187, 353
SMTP Server 185
SSL 185
STARTTLS 185
SUBSCRIBE 187
Subscribe URL 185
UNSUBSCRIBE 187
Blacklist
Address 299
Blacklisted users 299

# - C -

Cache 68
Caching IPs 68
Calendar 125
Calendar & Scheduling 111
Calendar options
BES 179
BlackBerry Enterprise Server 179
Resetting the BlackBerry calendar 179
Slow Sync 179
Catalog control 506
Catalog Editor 478
Certificates 121, 309, 310, 313, 316
SSL 320
Using third-party 320
WorldClient 320
Certification 294, 296
Certification Service Providers 294, 296
Changes in MDaemon 15
Changing WorldClient's Port Setting 115
Choosing your account database 411
Clear message counts at startup 193
Closing the RAS session 92
Collecting stored SMTP mail 57
ComAgent 111
Composite Log 101
Configuring
Domain Gateways 458
DomainPOP Settings 81
IP Cache 68
IP Screen 302
IP Shield 273
MDaemon remotely 132
ODBC Data Source for a List 451
RAS Settings 92
Connection
attempts 92
Profile 94
Connection Window 36
Content Filter 210
Administrators 223, 227
Editor 212
Recipients 227
rules 218
Content Filter & SecurityPlus 210
Content Filter Editor 212

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Content-ID header 200
Control 504
Converting Headers 70
Cookies 116
Copying mail before parsing 92
CRAM-MD5 46
Create Rule Dialog 218
Creating
  Auto Response Scripts 393
  New Content Filter Rule 214
  New ODBC Data Source 414
  New System Data Source 453
  ODBC data source 414
  Site Policy 337
Creating and Using SSL Certificates 320
Cryptographic
  Signing 284, 289
  Verification 284, 285
CSP 294, 296
Customizing the Queue/Statistic Manager 500

# - D -

Daemon 251
Data Source 412, 414
Database Options 411, 412
Date header 200
Deduping Mail 85
Default Domain
  Archival 59
  Delivery 43
  Dequeue 57
  DNS 51
  Domain 41
  FQDN 41
  IP 41
  Name 41
  Overview 40
  Ports 49
  Pruning 61
  Servers 46
  Settings 41
  Threads 55
  Timers 53
  Unknown Mail 63
Default headers 85
Defining Content Filter administrators 223
Deleting mail 88
Deleting POP mail after collection 83
Delivery 43
Delivery based on non-address info 90
Delivery Status Notification message 488
Delivery Times 145
Dequeue 57
Dequeue AUTH 57
Dequeuing 466
Dequeuing Gateway Messages 466
Dequeuing Mail 57, 59, 466
Dialup only if Remote Mail is waiting 93
Dialup Profile 94
Dialup Settings 92, 93
Digest 441
Disk 197
Disk Space
  Low 197
  Monitoring 197
  Settings 197
disk space limits 469
Display 30
display font 193
DK & DKIM signing 289
DK & DKIM verifying 285
DKIM 284, 294, 296
  DNS 289
  Options 292
  Private Keys 289
  Public Keys 289
  Selectors 289
  Signatures 285
  Signing 289
  Verification 285
DNS
  Black List Exceptions 266
  Black Lists 264
  Server 51
  Server IP Address 51
DNS Black Lists 265
DNS-BL 264
  Hosts 265
  Options 267
  White List 266
Documents Folders 74
Domain Administrators 377
Domain Gateways 322, 323, 458
Domain Manager 108
Domain Name Replacement 87

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Domain Policy 174
Domain Settings 460
Domain Sharing 64
Domain Signatures (text/html) 73
Domain Signatures (text/plain) 72
DomainKeys
  DNS 289
  Overview 284
  Private keys 289
  Public keys 289
  Selectors 289
  Signatures 285
  Signing 289
  Verification 285
DomainKeys Identified Mail 284, 285, 289
DomainPOP 81
  Account 83
  Foreign Mail 89
  Mail Collection 81
  Name Matching 90
  Parsing 85
  Processing 87
  Routing Rules 88
  Security 92
DomainPOP Mail Collection 81
Domains 41, 335
  Administrators 377
  BES 174
  BIS 185
  BlackBerry Enterprise Server 174
  BlackBerry Internet Service 185
  Creating 108
  Default Domain Overview 40
  Default FQDN 41
  Default IP 41
  Default Settings 41
  Deleting 108
  FQDN 108
  Renaming 108
  Sharing 64
  Trusted 279
Download
  Limits 83, 366
  Size Limits 83, 366
DSN message 488
DSN Options 488
Duplicate mail 85
Dynamic Authentication 425
Dynamic Screening 306

# - E -

Edit Rule 218
Editing
  Domain gateways 458
  Headers 70
EICAR virus test messages 233, 235
Email SSL 309, 310
Enabling
  DomainPOP Mail Collection 83
  Public Folders 75
  WorldClient Server 116
Enterprise Activation 162
Enterprise Activation password 351
Erasing a BlackBerry device 351
ESMTP 46, 57, 466
ESMTP SIZE command 46
ESMTP VRFY commands 46
ETRN 57, 466
ETRN Dequeue 466
Event Log 102
Event Scheduler 145, 148, 152
Event Tracking Window 30
Exception List
  Autoresponders 391
Excluding addresses from filtering 256
Exclusion List 256
EXPN 46
expressions 218
Extracting Attachments 142, 349

# - F -

Faxing 127
File Attachments 349
File Compression 228
Files
  Accessing from a BlackBerry device 175
Filtering mail 353
Filtering Messages 210, 212
Filtering Spam 241, 242, 262
Filters 356
Fingering an ISP 57
Fixes 199
Flagging Spam 242, 262, 265

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.

Flags 77
Folder access rights 79
Folders 74, 77, 353
Footer 445
Foreign Mail 89
Forwarding 362, 470
Forwarding Mail 88, 362
Free/Busy Server Options 126

# - G -

Gateway
  Domain Settings 460
  Domains 458
  Editor 459
  Options 470
  Quotas 469
Gateway Domain Editor
  Active Directory 461
  Domain Settings 460
  ESMTP ETRN 466
  LDAP 461
  Mail Forwarding 470
  Minger 461
  POP/IMAP 468
  Quotas 469
  Verification 461
Gateway Editor 459
Gateways 322, 323, 458
  Address Verification 422
  Verification 422
GatewayUsers.dat file 461
General Email Controls 509
Getting Help 22
Global
  Administrators 377
  Auth 280
  Blacklist 299
Glossary 522
Greylisting 330
Groups 349, 420
  Adding accounts 420
GUI 30, 193

# - H -

HashCash 333
Header 445
Header Translation 70
  Exceptions 71
Headers 70, 85, 200
Help 22, 30
Help with WorldClient 115
Heuristics 242
Holding Queue 484
Host Screening 304
Hosts 265
HTTPS 121, 136

# - I -

IIS 116, 118
  Running WebAdmin under 138
IMAP 49, 53, 343, 345
  Filters 356
  Folder access rights 79
  Folders 77
  Mail Rules 356
IMAP Folders 353
IMAP message flags 77
IMAP Spam Folder 267
Importing
  Accounts 423, 425
  Accounts From a Text File 423
Inbound Session Threads 55
Installing Domain Gateway 458
Instant Messaging 111, 124
Integrated Accounts
  BES 176
  BIS 187
  BlackBerry Enterprise Server 176
  BlackBerry Internet Service 187
  Slow Sync 176
Integration 425
Interface 30
Intranet
  Accessing from a BlackBerry device 175
Introduction 12
IP Cache 68
IP Screening 302
  Automatic 328
IP Shield 273
IP Shielding 273
ISP LAST command 83
ISP Logon Settings 94

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

ISP POP Accounts 83
IT Policies 167
Per Domain 174

# - L -

LAN Domains 335
LAN IPs 336
Latency 53
LDaemon 96
LDaemon LDAP Server 96
LDAP 96, 97, 406, 448
Base Entry DN 406, 448
Port (Gateway) 461
Root DN 406
Root DSE 406
Root Entry DN 448
Server (Gateway) 461
Verification (Gateway) 461
LDAP Database Option 411
LDAP Options 97
LDAP/Address Book Options 96, 97
Learning
Bayesian 249
Leaving mail at ISP 83
Lightweight Directory Access Protocol 96
Limiting bandwidth 325
Limits 83, 366
Linking Attachments 142, 349
List Moderation 440
List Routing 442
List Security 440
literals 218
Local Queue prepost processing 490
Locking the MDaemon interface 34
Log
Archiving 103
Backups 103
Maintenance 103
Log Mode 99
Log Options 104
Log Page 497
Logging 99
BES 179
BIS 189
BlackBerry Enterprise Server 179
BlackBerry Internet Service 189
Composite Log 101
Event Log 102
Log Mode 99
Log Options 104
Maintenance 103
Windows Event Log 102
Logging in to WorldClient 115
Logon Name 94
Logon Settings 94
Loop Detection 53
Low Disk Space 197

# - M -

Mail
Custom Queues 486
Filters 356
Forwarding 362, 470
Pruning 366
Queues 74
Rules 356
Mail quotas 419
Mail Release 57, 59
Mail Schedule 148
Mail Services 345
Mailbox 349
Mailing List and Catalog Control 506
Mailing Lists
Active Directory 448
ALL_USERS list macro 433
ALL_USERS:<domain> list macro 433
Creating 430
Digest 441
Digest toggle 433
Members 433
Membership Type 433
Moderating lists 440
Modifying 430
Notifications 444
ODBC 450
Options 431
Post Only toggle 433
Public Folder 447
Read Only toggle 433
Routing 442
Security 440
Subscriptions 436
Support Files 445
Using Active Directory with 448

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Main Window 30, 193
Maintenance 103
Manager 340
Managing Domains 108
Marking Messages as Spam 265
Max
  domains listed 193
  messages 469
  number of accounts shown 193
  number of log lines displayed 193
Maximum Message Hop 53
MDaemon 310
  Upgrading 26
MDaemon 11 15
MDaemon 12 15
MDaemon and Proxy Servers 519
MDaemon and Text Files 504
MDaemon CA 320
MDaemon Features 12
MDaemon GUI 30
MDaemon Messaging Server 12
MDaemon Technical Support 22
MDaemon's SMTP Work Flow 37
MDS Connection Service 175
MDSpamD 251
MDStats Command Line Parameters 501
MDStats.ini File 500
Meetings 125
Members 433
Menu 30
Message Certification 294, 296
Message Filters 356
Message Flags 77
Message Macros 225
Message-ID header 200
metacharacters 218
Migrating Account DBase to ODBC 412
Minger 64, 422, 461
Mirroring to Windows Address Book 418
Miscellaneous 202
Moderating lists 440
Modify Rule 218
Modifying an Existing Content Filter Rule 218
Monitoring Active Directory 404
Multiple Domains 64
MultiPOP 150, 345, 369

# - N -

Name Matching 90
Network Resource Access 205
Network Shares 205
New Account Defaults 380, 383, 385, 387, 420
  Mailbox 380
New accounts 380, 385, 387
New Features 15
Notepad 504
Notes 376
Notifications 224, 444
  Delivery Status Notification 488
  DSN 488

# - O -

ODBC
  Account Database 412
  Data Source 412, 414
  Database Option 411
  Mailing Lists 450
  Selector Wizard - Account Database 412
  System Data Source 451
ODMR 49, 57, 466
Old Mail Pruning 366
On-Demand Mail Relay 57, 466
On-Demand Mail Relay (ODMR) 59
Options 400
  Autoresponders 392
  BES 179
  BlackBerry Enterprise Server 179
  Free/Busy Services 126
Order of processing 37
Outbound Session Threads 55
Outbreak Protection 236
Outlook Connector 345
  Activating 409
  Adding Users 410
  Authorizing Users 410
  Contact Folders 409
  Generating Shared Folders 409
  Options 409
  Removing Users 410
  Restricting Users 409
  Users 410

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Outlook Connector for MDaemon 408
Overview 12

# - P -

Parsing
  Deduping Mail 85
  List of parsed headers 85
  Names preceeding email address 90
  parsing 85
  Skipping over 85
Password 94
  Activation 351
  BlackBerry device activation 351
  Enterprise Activation 351
  ISP POP accounts 83
  POP mail account 83
Performance Enhancements 15
Per-user flags 77
Policies 167, 351
  Account specific 351
  ActiveSync 156, 159
  Per Domain 174
  Sending to a BlackBerry device 351
Policy Rules 167
POP Access 468
POP Before SMTP 278
POP DELE command 46
POP mail collection 81
POP Server 83
POP3 345
Ports 49
  SSL 313, 316
Post Connection 95
Postmaster 93
  informed when dialup fails 92
  receiving summary of non 89
Precedence bulk header 200
Preferences
  Disk 197
  Fixes 199
  GUI 193
  Headers 200
  Miscellaneous 202
  MultiPOP 150
  Quotas 419
  Servers 46
  System 195
  WAB 418
pre-process list mail 195
Pre-processing 490
Preventing duplicate messages 85
Priority Mail 66
Process 95
Processing 87
Profile 94
Programs 95
Protection
  Against backscatter 322, 323
Proxy Servers 519
Pruning 61, 366
Public Catalog 478
Public Folders 74, 75, 77, 371
  Mailing Lists 447
Public IMAP Folders 74
Push mail 353

# - Q -

QSND 57
Queue and Statistics Manager 491
Queue Page 492
Queue pre-processing 490
Queued Mail 30
Queues 74, 482, 487
  Custom 486
  Restoring default locations 487
Quotas 366, 385, 419, 469

# - R -

RAS Dialup 92
  Dialup Settings 92
  Engine 92
  Settings 92
RAS Dialup Settings
  ISP Logon Settings 94
  Post Connection 95
RAW
  Bypassing the Content Filter 509
  Message Specification 509
  Sample messages 509
  Special fields supported by 509
RBL 264
RBL Hosts 265

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Real-time Black Lists 264
Received header 85
Recipients 227
Refusing non 89
Regular Expressions 218
Rejecting Spam 242, 262
Relay Control 271
Relay Settings 271
RelayFax
  Integration with WorldClient 127
Release Notes 15
Reminders 125
Remote Access and Control 504, 506, 509
Remote Address Verification 422
Remote Configuration 132, 134
Remote LDAP server 461
Remote Mail Scheduling 145
Remote verification of addresses 461
Reply-To header 200
Report Page 499
Reporting 261
Requirements 12
Resetting the calendar 179
Resources 30
Restore 487
Restoring the BES database from a backup file 177
Restricting attachments 223
Restriction 364
Resynchronizing a device 351
Retrieving stored SMTP mail 57
Retry 482
Retry Queue Settings 482
Return-Receipt-To header 200
Reverse Lookup 275
Root DN 406, 448
Root DSE 406
Route Slips 518
Routing 442
Routing mail to various users 88
Routing Rules 88
Rules 88, 356
  BES Policy 167
  BlackBerry device policy 167
  BlackBerry Enterprise Server policy 167
  Policy 167
Running WebAdmin under IIS 138
Running WorldClient under IIS6 118

# - S -

Saving Mail 92
Scanning for viruses 231
Scheduler 145, 260
  AntiVirus updating 151
  Custom queue scheduling 145
  Event Scheduling 145
  Remote Mail Scheduling 145
  SecurityPlus updating 151
  Spam Filter updates 260
Scheduling AntiVirus Updates 152
Screening 208, 302
Screening Hosts 304
Secure Sockets Layer protocol 121, 309, 310, 313, 316, 319, 320
Security 92, 425, 440
  Backscatter Protection 323
  Backscatter Protection - Overview 322
  BATV 322, 323
  Dynamic Screening 306
  Features 208
  Settings 208
SecurityPlus 210
  Configuring updater 233, 235
  EICAR test message 233, 235
  Malware 233, 235
  Quarantine 231
  Scheduler 151, 233, 235
  Testing 151, 233, 235
  Updater 151, 233, 235
  Urgent Updates 151, 233, 235
  Viewing update report 233, 235
  virus scanning 231
SecurityPlus for MDaemon 210, 231, 236
Semaphore Files 512
Send & Collect Mail 145
Sender Policy Framework 282
Sender-ID 294, 296
Sending mail to various users 88
Server
  WorldClient 111
Server level administrators 377
Servers 46
Service 205
Service books
  Resending 351

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Services
BES 166, 179
BlackBerry Enterprise Server 166, 179
MDaemon BES 166
Stopping when MDaemon stops 179
Session Threads 55
Session Window 36
Setting a Domain's Policy 174
Setting Download Size Limits 83
Setting IMAP Folder Flags 75
Setting parameters for mail delivery 88
Setting the number if dialup attempts 92
Setting up
Account Defaults 380, 387
Account Template Strings 380, 387
Auto Response Scripts 393
Default Account Quotas 385
Domain Gateways 458
DomainPOP Mail Collection 81
Global Blacklist 299
IP Screen 302
IP Shielding 273
RAS 92
Remote configuration 132
Web Access Defaults 387
Shared Folders 74, 75, 371
Shared IMAP Folders 75, 77
Shared user folders 79
Sharing Domains 64
Sharing mail folders 74
Shortcut Menu 34
Signaling ISP to dequeue mail 57
Signature
Account 375
Signatures
Domain 72, 73
Signing 289
Signing Messages 284
Simple Reporting 261
Site Policy 337
Site Security Policy 337
Skipping 85
Slow Sync 176
Synchronizing a specific device 351
SMTP Authentication 280
SMTP call-back 422
SMTP call-forward 422
SMTP Connection Window 36
SMTP RCPT threshold 328
SMTP Work Flow 37
Space 197
Spam
Addresses 270
Automatic white listing 253
Bayesian Learning 245
Black List 259, 262
Classification 245
Deleting 242, 262
Directory 245
False negative classification 245
False positive classification 245
Filtering 242, 253, 257, 258, 259, 262
Inserting tag into subject 242
Non-spam directory 245
Rejecting 242, 262
Reporting 261
Required score 242
Scoring 242
Simple Reporting 261
Threshold 242
Traps 270
White List 257, 258, 262
Spam Assassin 251
Spam Filter 241, 267
Bayesian Auto-learning 249
Exclusion List 256
MDSpamD 251
Reports 261
Spam Daemon 251
Spam Filtering 262
Updates 260
using and external spam daemon 251
White List 256
Spam Folder 267
Spam Traps 270
SpamD 251
SPF 282, 294, 296
SRP 166
SSL 121, 136
BIS 185
BlackBerry Internet Service 185
MDaemon 310
STARTTLS 319
TLS 319
WebAdmin 316
White List 319

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

SSL 121, 136
WorldClient 313
SSL & Certificates 121, 309, 310, 313, 316, 320
SSL Certificates 320
SSL Ports 49, 313, 316
Stamps 333
Starting WorldClient 115
STARTTLS 309, 310, 319
BIS 185
BlackBerry Internet Service 185
startup 193
Statistics 30
Status
BlackBerry 166
STLS 309, 310
Subaddressing 356
Subscribe 436, 438
Subscribing To Mailing Lists 438
Subscriptions 436
Support 22
Support Files 445
Suppressed users 299
Suppression 445
Synchronization 111
Synchronization options
BES 179
BlackBerry Enterprise Server 179
Calendar 179
Slow Sync 179
When activating 179
SyncML 191
Configuring your client 191
System 195
System account email address 195
System Data Source 414
System Requirements 12
System Service 205
system tray 193

# - T -

tagged expressions 218
Tarpit Settings 328
Tarpit Threshold 328
task bar 193
Task reminders 125
TCP 49
Technical Support 22
Template Macros 383
Templates 380, 383
Text Files 504
Third-party Certificates 320
Threading 55
Threads 55
Threshold
Spam rejection 242
Throttling 326
Timeout 53
Timers 53, 145
TLS 309, 310, 319
Toolbar 30
Tray Icon 34
Trusted
Domains 279
Hosts 279
Trusted Domains 271

# - U -

UDP 49
Undeliverable Mail 482
Unknown Local Mail 63
Unlocking the MDaemon interface 34
Unsubscribe 436
Updates 260
Updating virus definitions 151
Upgrading MDaemon 26
Urgent Updates 151
User Folders 74
User Page 495
Userlist.dat Database Option 411
Using Regular Expressions 218

# - V -

VBR 294, 296
Verification
Gateways 461
Remote Address 461
via Active Directory 461
via GatewayUsers.dat file 461
via LDAP 461
via Minger 461
Verifying DomainKeys 285
Verifying Signatures 284

*Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.*

Verifying SRP Credentials 166
Version 11 15
Version 12 15
Virus
  Updater 151
Virus:Protection 210
Viruses 236
Vouch-By-Reference 294, 296
VRFY 46, 422

# - W -

WAB 418
Web Access Defaults 387
Web Access Permissions 346
Web configuration 132
Web Server 116
WebAdmin 132, 134, 346
  Running under IIS 138
  SSL 316
WebAdmin SSL 136
Welcome File 445
Welcome message subject header 200
What's New? 15
White List 241, 262
  DNS-BL 266
  Spam Filter 256
  SSL 319
  TLS 319
White List auto 253
White List from 258
White List to 257
Windows Account Integration 425
Windows Address Book 418
Windows Service 205
Wiping a BlackBerry device 351
WorldClient 111, 346
  Address Book 129
  Calendar 125
  ComAgent support 124
  Date Format 129
  Default Language 129
  Default Theme 129
  Domain Options 124, 129
  Free/Busy Options 126
  Getting Help 115
  Instant messaging 124
  Logging in 115
  Meetings 125
  Options 129
  RelayFax integration 127
  Reminders 125
  Server Properties 116
  Signing in 115
  SSL 121, 309, 313
  SSL & Certificates 320
  Starting WorldClient 115
  SyncML 191
  Task reminders 125
  Web Server 116
  WorldClient SSL 121, 309
WorldClient Documents Folders 74
WorldClient Help 115

# - X -

X-RBL-Warning headers 200
X-type headers 200

Copyright © 1996-2012. All rights reserved. Alt-N Technologies, Ltd.